HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

DIPLOMARBEIT

Herr Ing.
Michael Sandro Erhart

Konzept und prototypische Umsetzung von Maßnahmen zur Verbesserung der Client-Sicherheit von Geräten mit EOL-Betriebssystemen

Mittweida, 2017

Fakultät für Angewandte Computer- und Biowissenschaften

DIPLOMARBEIT

Konzept und prototypische Umsetzung von Maßnahmen zur Verbesserung der Client-Sicherheit von Geräten mit EOL-Betriebssystemen

Autor:
Herr Ing.

Michael Sandro Erhart

Studiengang:
Technische Informatik

Seminargruppe:
KT11wIA-F

Erstprüfer:
Prof. Dr.-Ing. Uwe Schneider

Zweitprüfer:
Ing. Mag. Arthur Meßner

Einreichung:
Mittweida, 31. Mai 2017

Verteidigung/Bewertung:
Mittweida, 2017

Faculty Applied Computer Sciences &
Biosciences

DIPLOMA THESIS

Concept and prototypical implementation of measures for improving client security of EOL-OS clients

author:
Mr. Ing.

Michael Sandro Erhart

course of studies:
Computer Engineering

seminar group:
KT11wIA-F

first examiner:
Prof. Dr.-Ing. Uwe Schneider

second examiner:
Ing. Mag. Arthur Meßner

submission:
Mittweida, May 31, 2017

defence/ evaluation:
Mittweida, 2017

Bibliografische Beschreibung:

Erhart, Michael Sandro:
Konzept und prototypische Umsetzung von Maßnahmen zur Verbesserung der Client-Sicherheit von Geräten mit EOL-Betriebssystemen. - 2017. - VII, 79, VIII S.
Mittweida, Hochschule Mittweida, Fakultät für Angewandte Computer- und Biowissenschaften, Diplomarbeit, 2017

Referat:

Die vorliegende Arbeit hat die Erstellung eines Konzeptes und die prototypische Umsetzung von Maßnahmen zur Verbesserung der Client-Sicherheit mit EOL-Betriebssystemen zum Ziel. Die Erstellung des Konzeptes basiert auf dem Beispiel der Tirol Kliniken GmbH. Im theoretischen Teil werden die Grundlagen zur IT-Sicherheit und das Gefahrenpotential betrachtet. Im praktischen Teil wird ein allgemeines Konzept ausgearbeitet, mit Hilfe dessen analysiert werden kann, inwiefern die EOL-Clients im Unternehmen geschützt sind und ob es weiterer Maßnahmen bedarf. Dies wird am Beispiel der Tirol Kliniken, mit besonderem Fokus auf McAfee Application Control, dargestellt.

Abstract:

The present thesis aims at drafting a concept and prototypically implementing measures for improving client security for EOL-OS clients. The concept is based on the example of the Tirol Kliniken GmbH (corporation for the administration of Tyrolean hospitals). The theoretical part details the basics of IT security and any potential risks. In the practical part, a general concept will be drafted. With the help of this concept, it will be possible to analyse how well EOL clients of the company are protected and if any further measures are required. This is outlined by taking the Tirol Kliniken as example, particularly focussing on McAfee Application Control.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACOnet	Austrian Academic Computer Network
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
BGBl	Bundesgesetzblatt
BS	Betriebssystem
BSDG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
bzw.	beziehungsweise
CASP	Critical Address Space Protection
CD	Compact Disc
CD-ROM	Compact Disc Read-Only Memory
CERT	Computer Emergency Response Team
COE	Consistent/Common Operating Environment
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service
DEP	Data Execution Prevention
DICOM	Digital Imaging and Communications in Medicine
DLL	Dynamic Link Library
DoS	Denial of Service
DSG	Datenschutzgesetz
EC	European Commission
EEG	Elektroenzephalografie
EG	Europäische Gemeinschaft
EKG	Elektrokardiogramm
EOL	End of Life
ePO	ePolicy Orchestrator
EU	Europäische Union
EWG	Europäische Wirtschaftsgemeinschaft
FAQ	Frequently Asked Questions
FTP	File Transfer Protocol
GTI	Global Threat Intelligence
GUS	Gemeinschaft Unabhängiger Staaten
HT	Haustechnik
HTTP	Hypertext Transfer Protocol
idgF.	in der geltenden Fassung
IDS	Intrusion Detection System
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
IP	Internet Protocol

ISMS	Informationssicherheitsmanagementsystem
ISO	Internationale Organisation für Normung
IT	Informationstechnik
ITK	Informations- und Telekommunikationstechnologie
KIS	Krankenhausinformationssystem
MP	Medizinprodukte
MPBV	Medizinproduktebetreiberverordnung
MPG	Medizinproduktegesetz
MT	Medizintechnik
MwSt	Mehrwertsteuer
NX	No Execute
o.Ä.	Oder Ähnliches
OS	Operating System
OSI	Open Systems Interconnection
p2p	Peer-to-Peer
PACS	Picture Archiving and Communication System
PC	Personal Computer
PDCA	Plan-Do-Check-Act
SMTP	Simple Mail Transport Protocol
SOE	Standard Operating Environment
SOP	Standard Operating Procedures
SPI	Stateful Packet Inspection
TB/s	Terabyte pro Sekunde
TCP	Transmission Control Protocol
URL	Uniform Resource Locator
USB	Universal Serial Bus
VASR	Virtual Address Space Randomization
VB	Visual Basic
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WLAN	Wireless Local Area Network
WSUS	Windows Server Update Services
z.B.	Zum Beispiel

Vorwort

Die vorliegende Arbeit wurde als Abschlussarbeit im Zuge des Fernstudienganges Technische Informatik an der Hochschule Mittweida verfasst.

Mein Dank gilt Herrn Prof. Dr.-Ing. Uwe Schneider für die Betreuung und Unterstützung bei dieser Diplomarbeit.

Weiters möchte ich mich bei meinem betrieblichen Betreuer Herrn Ing. Mag. Arthur Meßner bedanken, der mir immer mit gutem Rat zur Seite stand und bei unseren Gesprächen Anregungen zur Verbesserung meiner Arbeit gegeben hat. Ebenso möchte ich mich bei meinen Vorgesetzten Herrn DI (FH) Romed Giner, Bereichsleiter, und Herrn Dr. Georg Lechleitner, Abteilungsvorstand der Tirol Kliniken Informationstechnologie, für die Unterstützung seitens des Arbeitgebers und bei meinen Arbeitskollegen für ihre wertvollen Tipps und Bereitstellung von Informationen bedanken.

Mein besonderer Dank geht an meine Frau Verena, die mich während der Erstellung der Arbeit unterstützte und motivierte, meine Launen während der ganzen Studienzeit ertragen musste und die Arbeit Korrektur gelesen hat. Ebenso geht mein Dank auch an meine Eltern Anna und Hermann, die mich in allen meinen Lebenslagen unterstützen.

Aus Gründen der besseren Lesbarkeit wird in dieser Arbeit auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichwohl für beiderlei Geschlecht.

1 Einleitung

Die immer rasanter werdende technische Entwicklung, auch in Bezug auf Betriebssysteme und Programme, führt dazu, dass Unternehmen in größerem Ausmaße darauf achten müssen, dass ihre Clients mit einem noch gewarteten Betriebssystem betrieben werden und auch ausreichend geschützt sind.

Gerade deswegen ist es wichtig, die vorhandene Infrastruktur auf etwaige Schwachstellen zu überprüfen und diese zu beseitigen.

1.1 Motivation

Besonders in klinischen Unternehmen, wie den Tirol Kliniken, in dessen IT-Abteilung der Autor dieser Arbeit tätig ist, ist eine ständige Aktualisierung der Clients eine herausfordernde Aufgabe. Wie später noch dargestellt wird, gibt es in einer solchen IT-Umgebung auch Clients, die aus verschiedensten Gründen nicht verändert oder aktualisiert werden dürfen. Solche Clients – die oft mit einem End Of Life (EOL) Betriebssystem (ein Betriebssystem, dass durch den Hersteller keine Updates mehr erhält oder gewartet wird) versehen sind – bedürfen natürlich eines zusätzlichen Schutzes, damit sie (und auch das Netzwerk) vor möglichen Gefahren geschützt werden. Da nach der Client-Umstellung von Windows XP auf Windows 7 noch zahlreiche Rechner übrigblieben, die nicht umgestellt werden konnten, muss nun für diese Rechner eine zufriedenstellende Lösung gefunden werden.

1.2 Zielsetzung

Das Ziel dieser Arbeit ist es, Ansätze zur Verbesserung der Client-Security von EOL-Betriebssystemen zu erläutern. Daher werden im theoretischen Teil zuerst die Grundlagen in Bezug auf Sicherheit und Gefahren erläutert. Im praktischen Teil wird zuerst ein Konzept erarbeitet, wie eine IT-Umgebung in Bezug auf die Clients und die vorhandenen Schutzmaßnahmen analysiert werden kann. Dadurch können anschließend verschiedene Möglichkeiten, wie die unzureichend geschützten EOL-Rechner besser abgesichert werden können, ausgearbeitet werden.

1.3 Kapitelübersicht

Kapitel 2 widmet sich den Grundlagen der IT-Sicherheit: den Sicherheitszielen, dem ISO/OSI Modell und dessen Sicherheitsaspekte sowie den rechtlichen Grundlagen, besonders in Bezug auf eine IT-Infrastruktur in einer klinischen Umgebung. Des Weiteren wird das Gefahrenpotenzial dargestellt; einerseits die Gefährdungskategorien anhand des IT-Grundschutzkataloges (BSI, Deutschland), andererseits die spezifischen Gefahrenquel-

len. Schlussendlich wird noch auf die allgemein vorhandenen Schutzmaßnahmen für Clients eingegangen.

In Kapitel 3 wird zuerst ein allgemeines Konzept ausgearbeitet, anhand dessen Unternehmen ihre IT-Infrastruktur dahingehend analysieren können, wie ihre Clients (besonders EOL) geschützt sind und ob es weiterer Maßnahmen bedarf. Anschließend wird dies durch eine IST-Analyse der Tirol Kliniken, die auf diesem Konzept basiert, und einer darauf folgenden SOLL-Analyse, inwiefern die kritischen Rechner auf einen zufriedenstellenden Standard gebracht werden können, dargestellt.

Kapitel 4 widmet sich dann noch dem Programm McAfee Application Control, das in den Tirol Kliniken – wie in Kapitel 3 festgestellt wird – zum Schutz von EOL-Clients zum Einsatz kommen soll.

2 Grundlagen

Als Grundlage für die Ausarbeitung dieser Arbeit werden im folgenden Kapitel sowohl die Sicherheit im Bereich der IT (Sicherheitsziele, ISO/OSI Modell, Rechtliche Grundlagen) als auch das Gefahrenpotential allgemein (Gefährdungskategorien, Gefahrenquellen) behandelt. Auch die aktuelle Lage in Bezug auf Gefahrenquellen wird kurz erläutert. Anschließend wird noch auf die möglichen Schutzmaßnahmen für Clients eingegangen.

2.1 Was ist Sicherheit allgemein?

Wie viele abstrakte Worte besitzt auch „Sicherheit“ mehrere Bedeutungen. Für die vorliegende Arbeit treffen allerdings die Definitionen „Zustand des Sicherseins, Geschütztseins vor Gefahr od. Schaden; höchstmögliches Freisein von Gefährdungen“ und in weiterer Folge „das Freisein von Fehlern u. Irrtümern; Zuverlässigkeit“ (Duden Universalwörterbuch, s.v. Sicherheit) am ehesten zu. Dieser Zustand kann nicht nur auf Lebewesen oder Dinge, sondern auch auf abstrakte Gegenstände bezogen werden.

Schon immer spielte Sicherheit eine große Rolle in den verschiedensten Lebensbereichen – Sicherheit zuhause, in der Gemeinschaft, im beruflichen Leben, wirtschaftlich gesehen. In der heutigen, hoch entwickelten und industrialisierten Zeit nimmt Sicherheit einen immer größeren Stellenwert ein und wird in vielen Bereichen durch verschiedenste Organisationen (ISO, EC, …) immer genauer definiert und bestimmt. Besonders in technischen Bereichen, wie der IT, wird großer Wert auf *Sicherheit* gelegt.

2.2 Sicherheit im Bereich der IT

In fast allen denkbaren Bereichen spielt Informations- und Kommunikationstechnologie eine immer größere Rolle. Die Digitalisierung der Kommunikation und Vernetzung verlangt dabei aber auch nach *Sicherheit*. Hier kommt die *IT-Sicherheit* ins Spiel. Auch dafür gibt es zahllose Versuche von Definitionen. Atencio Psille & Eschweiler versuchen, die Definition von IT-Sicherheit auf mehreren Seiten herzuleiten (unter Einbeziehung der allgemeinen IT-Sicherheitsziele) und gelangen zu folgendem Schluss:

> *„Der Begriff „IT-Sicherheit“ umfasst die für die Erbringung von Informations- und Kommunikationsleistungen unmittelbar erforderlichen Komponenten, die andauernde Gewährleistung definierter Eigenschaften dieser Komponenten und die in diesem Zusammenhang auftretenden relevanten und unerwünschten Ereignisse sowie die Maßnahmen zu deren Behandlung.*
>
> *Zielsetzung der IT-Sicherheit ist die Gewährleistung bestimmter Eigenschaften von IT-Komponenten und der von ihnen gebildeten IT-Systeme*

> *sowie der in ihrem Zusammenhang angebotenen Dienste. Die zum Erreichen der Zielsetzungen eingesetzten Mittel und Methoden zählen ebenfalls zu den Bestandteilen der IT-Sicherheit.“ (Atencio Psille & Eschweiler 2006:23)*

Eckerts (2012:1) Definition von IT-Sicherheit ist etwas enger gefasst und beschreibt, dass es die Aufgabe der IT-Sicherheit ist „Unternehmen und deren Werte (Know-How, Kundendaten, Personaldaten) zu schützen und wirtschaftliche Schäden, die durch Vertraulichkeitsverletzungen, Manipulationen oder auch Störungen der Verfügbarkeit von Diensten des Unternehmens entstehen können, zu verhindern.“ Da es unmöglich ist, sämtliche denkbaren Angriffe zu verhindern, sind auch Konzepte und Maßnahmen zur Verringerung solcher Angriffe Teil der IT-Sicherheit. Auch die Erkennung von Schwachstellen und deren Beseitigung sowie die angemessene und rasche Reaktion auf tatsächlich eingetretene Schäden werden dabei mit umfasst. (Vgl. ibid.)

IT-Sicherheit inkludiert jedoch auch im weiteren Sinne die Verbesserung der allgemeinen Sicherheit. Besonders gemeint sind hierbei zum Beispiel kritische Infrastrukturen (Kraftwerke, Transportleitsysteme etc.), für deren Überwachung Sensoren Umgebungsdaten erfassen, Daten austauschen oder auch den Ablauf/den Betrieb überwachen. So kann unter anderem teilweise völlig automatisiert in kritische Abläufe eingegriffen werden. Da solche Daten zumeist dem Datenschutz unterliegen, somit vertraulich zu behandeln sind und oft auch als sensible Daten vor Manipulation geschützt werden müssen, sind IT-Sicherheitskonzepte die Grundlage solcher Anwendungen. (Vgl. ibid. 1f)

In einem IT-System („dynamisches technisches System mit der Fähigkeit zur Speicherung und Erarbeitung von Informationen“ [Eckert 2012:3]) können verschiedene Arten von Sicherheit festgelegt werden (nach Eckert 2012:6 und Schneider 2012:480), die sich am leichtesten anhand der verschiedenen englischen Begriffe, die es für das deutsche Wort *Sicherheit* gibt, unterscheiden lassen:

Funktionssicherheit (engl. *safety*):

Ist ein System funktionssicher, so läuft es unter (normalen) Betriebsbedingungen reibungslos, also so, wie es soll. Das heißt, die realisierten Funktionen stimmen mit den definierten Soll-Funktionen überein. Der Begriff *safety* wird für unbeabsichtigte Ereignisse verwendet.

Informationssicherheit (engl. *security*):

Unter Informationssicherheit versteht man die Eigenschaft eines funktionssicheren Systems, nur jene Systemzustände anzunehmen, bei der keine unautorisierte Informationsveränderung herbeigeführt wird. *Security* ist also der Schutz vor beabsichtigten Ereignissen.

Während Schneider Datensicherheit und Datenschutz zu *security* zählt, separiert sie Eckert (vgl. 2012:6) davon als *protection* und *privacy*:

> **Datensicherheit (engl. *protection*):**
>
> Ist ein IT-System datensicher, so nimmt das funktionssichere System nur jene Systemzustände an, die einen unautorisierten Zugriff auf Systemressourcen und Daten verweigern. Dies inkludiert insbesondere auch die Datensicherung (engl. *backup*).
>
> **Datenschutz (engl. *privacy*):**
>
> Der Begriff Datenschutz umfasst im engeren Sinne „die Fähigkeit einer natürlichen Person, die Weitergabe von Informationen, die sie persönlich betreffen, zu kontrollieren." (Ibid.)

Aus diesen Definitionen lässt sich nun feststellen, dass die Informations- und Datensicherheit eines IT-Systems ständig überprüft und angepasst werden muss, da sich Systemeigenschaften über die Zeit ändern können. Weiters kann abgeleitet werden, dass die Funktionssicherheit die Grundlage für Informations- und Datensicherheit eines jeden Systems darstellt. (Vgl. ibid.)

Die Begriffe *Verlässlichkeit* (engl. *dependability*), also die Eigenschaft „keine unzulässigen Zustände anzunehmen", und *Zuverlässigkeit* (engl. *reliability*) der Funktion, gehen mit dem Begriff der Funktionssicherheit einher und können als Grunderwartung an ein IT-System definiert werden. (Vgl. ibid.)

2.2.1 Sicherheitsziele

In der IT-Sicherheit gibt es mehrere Grundziele, die allgemein anerkannt sind. Hierbei handelt es sich um Schutzziele, die für das Erreichen und der Einhaltung der Informationssicherheit definiert sind (und somit auch zum Schutz der Daten bzw. Informationen). Die drei grundlegenden Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit werden im Nachfolgenden näher definiert.

Mit der *Vertraulichkeit* (engl. *confidentiality*) soll gewährleistet werden, dass Daten nicht unautorisiert gelesen werden können, was durch Berechtigungen kontrolliert werden kann. Dies gilt sowohl für Datenzugriff als auch für Datenübertragung; juristische Anforderungen (personenbezogene Daten, ärztliche Schweigepflicht oder geheime Informationen) sind hierbei natürlich zu berücksichtigen. (Vgl. Eckert 2012:9f und Pohlmann & Blumberg 2004:86). In der heutigen Zeit, in der sowohl Individuen als auch Unternehmen sensible Daten geschützt haben wollen, solche Daten aber für viele (Marktrecherche, Konkurrenzdruck etc.) von hohem Interesse sind, kann der Verlust der Vertraulichkeit – also die Offenlegung oder Weitergabe solcher Daten – zu großem Schaden führen. (Vgl. IT-Grundschutz 1) Es ist auch nicht so leicht, Vertraulichkeit zu gewährleisten, denn: Wer

entscheidet, welche Personen oder Systeme Zugriff auf bestimmte Daten haben? Wenn jemand Zugriff hat, bedeutet dies, dass er für alles oder nur einen Teil autorisiert ist? Ist diese Person autorisiert, die Daten Dritten weiterzugeben? (Vgl. Pfleeger & Pfleeger 2007:10)

Die *Integrität* eines Systems (engl. *integrity*) ist dann garantiert, wenn es nicht möglich ist, die geschützten Daten, Programme, Hardware etc. unautorisiert und unbemerkt zu verändern. Verfälschte oder gefälschte Daten können zu Fehlbuchungen, Leistungserschleichungen oder Änlichem führen. Um die Datenintegrität zu gewährleisten, sind Lese- oder Schreibberechtigungen für Dateien bzw. Zugriffsberechtigungen für Personen zu vergeben, ähnlich der Vorgehensweise um Vertraulichkeit zu gewährleisten (Vgl. Eckert 2012:9, Pohlmann & Blumberg 2004:86, Datenschutz). Laut Welke & Mayfield (zit. n. Pfleeger & Pfleeger 2007:11f) kann Integrität in verschiedenen Bereichen auch unterschiedliche Bedeutungen haben („precise, accurate, unmodified, modified only in acceptable ways, modified only by authorized people, modified only by authorized processes, consistent"). Dabei können auch zwei oder mehrere dieser Eigenschaften Integrität bedeuten. Seit einigen Jahren spielt den IT-Grundschutz-Katalogen (Kapitel 1) zufolge auch der Teilbereich der *digitalen Identität* eine immer wichtigere Rolle (Zahlungsanweisungen oder digitale Willenserklärungen werden einer falschen Person zugerechnet etc.)

Durch die *Verfügbarkeit* (engl. *availability*) wird sichergestellt, dass Daten, Programme, Hardware und alle weiteren notwendigen Mittel zu dem Zeitpunkt oder innerhalb des bestimmten Zeitrahmens verfügbar oder funktionsbereit sind, an dem sie von autorisierten Subjekten benötigt werden (vgl. Eckert 2012:11f, Datenschutz). Dabei muss laut Pfleeger & Pfleeger (2007:12, übersetzt von M.E.):

- *„die Reaktion auf die Anfrage zeitnah erfolgen,*
- *die Ressourcen für den Vorgang müssen fair aufgeteilt sein, damit das autorisierte Subjekt nicht gegenüber Anderen bevorzugt wird,*
- *der Service oder das System sind einfach zu benutzen und auf die Art und Weise für die es bestimmt war,*
- *Die Fehlertoleranz sollte der Philosophie folgen, dass Hardware- oder Softwarefehler zu einer eleganten Beendigung des Service oder anderen Workarounds führen, anstatt abzustürzen und zu plötzlichem Datenverlust zu führen,*
- *Concurrency (also Gleichzeitigkeit) sollte kontrolliert werden: das heißt, dass simultaner Zugriff, Deadlock Management oder alleiniger Zugriff je nach Notwendigkeit unterstützt werden müssen."*

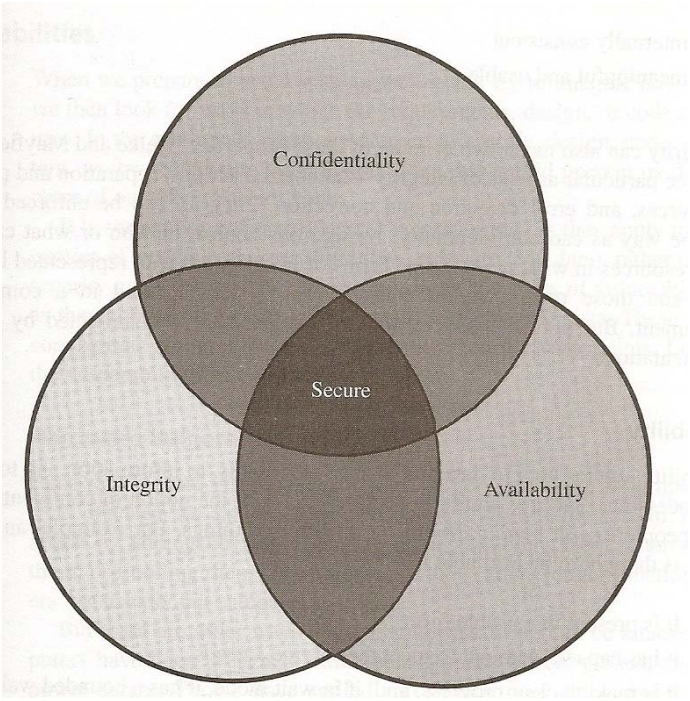

Abbildung 2-1: Beziehung der drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit (Quelle: Pfleeger & Pfleeger 2007:11)

Gerade in der heute digital abhängigen Arbeitswelt kann eine Beeinträchtigung oder gar ein Ausfall eines Systems weitreichende Folgen, darunter auch wirtschaftliche, haben.

Oftmals werden diese Schutzziele noch um die Folgenden erweitert:

Unter *Authentizität* (engl. *authenticity*) wird die Echtheit und Glaubwürdigkeit des Objektes bzw. Subjektes verstanden. Das heißt, die Herkunft von Daten und der Urheber derselben müssen korrekt zugeordnet werden können. In bestimmten Anwendungsfällen kann sich die Authentizität auch auf Programme oder Hardware beziehen (z.B. im elektronischen Zahlungsverkehr). Mithilfe der Authentifikation (Benutzernamen, Passwörter, biometrische Merkmale etc.) kann die Authentizität des Subjektes überprüft werden. (Vgl. Eckert 2012:8, Datenschutz)

Durch die *Verbindlichkeit* (engl. *non-repudiation*) soll ein Subjekt nicht durchgeführte Handlungen/Aktionen im Nachhinein abstreiten können. Dieses Grundziel ist insbesondere im Bereich des e-commerce und e-business äußerst wichtig, da dadurch die Rechtsverbindlichkeit von geschäftlichen Transaktionen wie Kaufverträgen gewährleistet werden kann. Genauso spielt die Verbindlichkeit auch in Mehrbenutzersystemen für die Zurechenbarkeit (engl. *accountability*) von beispielsweise Rechenzeit oder Gerätenutzung eine immer größere Rolle. (Vgl. Eckert 2012:12f)

Die *Anonymität* (engl. *anonymity*) gewinnt in den letzten Jahren, besonders im Hinblick auf zunehmend mehr vernetzte und auch mobile Systeme, immer mehr an Bedeutung. Unter diesem Ziel versteht man die Durchführung von Handlungen ohne dass die Identität preisgegeben werden muss. Eine abgeschwächte Form davon ist die Verwendung eines

Pseudonyms, die Identität ist also einem vertrauenswürdigen Dritten bekannt, nicht jedoch jedem beliebigen Kommunikationspartner. Die Anonymisierung zielt nicht nur darauf ab, personenbezogene Daten im engeren Sinne (Name, Geburtsdatum etc.) zu verschleiern, sondern auch solche Daten im weiteren Sinne: Aufenthaltsorte, Kommunikationsbeziehungen etc. (Vgl. Eckert 2012:13f)

2.2.2 Das ISO/OSI-Modell und dessen Sicherheitsaspekte

Mit der Entstehung und ständigen Erweiterung von internationalen Rechnernetzen entstand der Bedarf, Standards zu erarbeiten, die das Zusammenspiel von Geräten und Software unterschiedlicher Hersteller ermöglichten. Der von nationalen und internationalen Gremien erarbeitete OSI (Open Systems Interconnection) Standard normt die Datenkommunikation in offenen Systemen (Ein Verbundsystem, das „für alle Computer und Systembenutzer offen zugänglich ist, die zum System hin allgemein vereinbarte Anschlussbedingungen befolgen.“ [Schneider 2012:302]). (Vgl. Kerner 1992:20 und Schneider 2012:302)

Das OSI-Basisreferenzmodell (auch ISO/OSI-Modell) definiert eine Schichtenarchitektur für Kommunikationsprotokolle:

> *„Abstraktes, logisch-funktionelles Architekturmodell der Internationalen Standardorganisation ISO für die Datenkommunikation in offenen Systemen (OSI Open Systems Interconnection).“ (Schneider 2012:302)*

Die Schichten (Layer) des Modells folgen gewissen Regeln. So kann eine Einrichtung („Objekt in einer Schicht, das in der Lage ist, Informationen zu senden oder zu empfangen“ [Schneider 2012:303]) (1) nur mit Einrichtungen derselben Schicht kommunizieren, wobei diese Kommunikation aber nur über Dienste der nächsttieferen Schicht funktioniert, und darf (2) Nachrichten aus der nächsttieferen Schicht abfordern. (Vgl. Schneider 2012:303) Bei diesem Modell werden die zu übertragenden Daten aus dem obersten Application Layer durch alle Layer hindurch geschickt, bis sie durch das physische Medium zum Empfänger übertragen werden, wo die Daten wieder Layer für Layer bis hin zur obersten Schicht geschickt werden (vgl. Reed 2003:2).

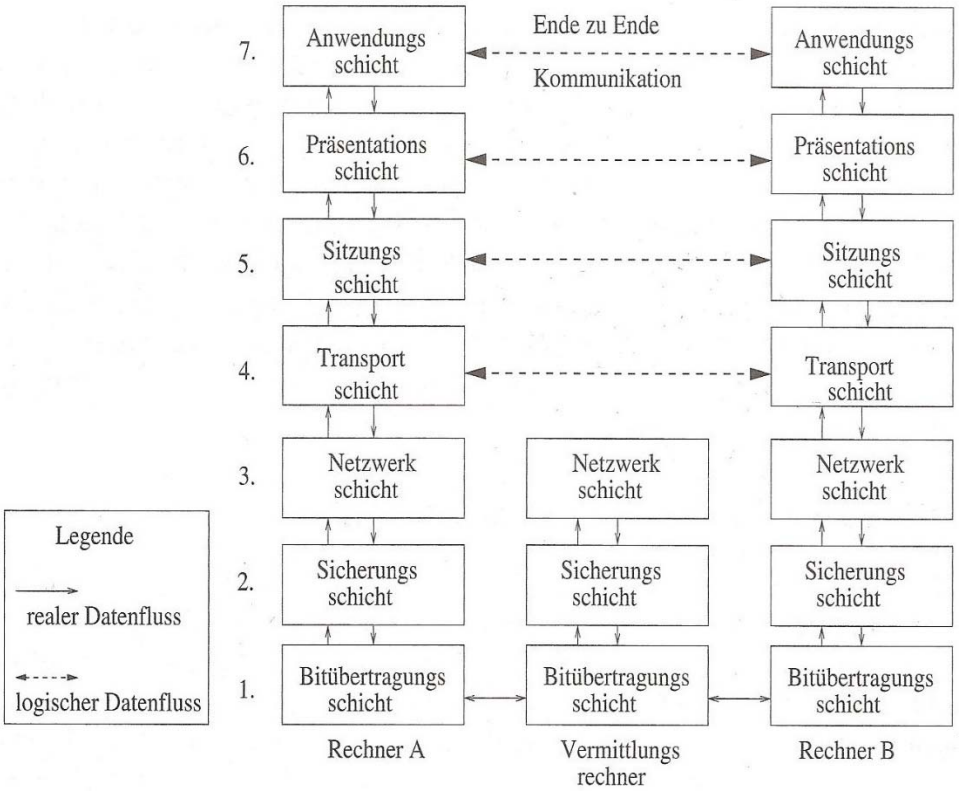

Abbildung 2-2: Die Schichten des OSI-Modells (Quelle: Eckert 2012:96)

2.2.2.1 Physical Layer

Der **Physical Layer** (*Bitübertragungsschicht*) hat es zur Aufgabe eine physikalische Verbindung zwischen zwei Kommunikationspunkten herzustellen und die Bitströme zu übertragen. Diese Schicht stellt die elektrischen, mechanischen und physischen Mittel für die Bitübermittlung zur Verfügung. Sie definiert die Charakteristika der physischen Verbindung (z.B. Spannung, Voltzahl, Anzahl der Pins, etc.) und regelt den Umgang mit verschiedenen Transportmedien wie Koaxialkabel, Lichtwellenleiter o.Ä. (Vgl. Eckert 2012:96ff und Schneider 2012:306f)

Der Physical Layer ist wohl der anfälligste Layer, denn er hängt nicht nur von der Logik der digitalen Welt, sondern auch von den Launen der Physik und der Natur ab. Schon etwas Simples, wie versehentlich einen Stecker ziehen, kann durchaus ernste Folgen für ein Netzwerk nach sich ziehen. Bei diesem Layer können noch „gewöhnliche“ Schutzmaßnahmen wie sicheres Versperren, Zugangsberechtigungen, Überwachung etc. eingesetzt werden. Bei einer kabellosen Übertragung muss auf eine gute Verschlüsselung der Daten geachtet werden, da ansonsten das Abhören leicht möglich wird. (Vgl. Reed 2003:6)

Schwächen: Stromausfall, Verlust über die Umgebungskontrolle, (physischer) Daten- und Hardwarediebstahl, (physische/r) Schaden und Zerstörung von Daten und Hardware, unau-

torisierte Veränderungen der funktionellen Umgebung (Datenverbindungen, Wechseldatenträger, Ressourcen hinzufügen/entfernen), … (Vgl. ibid)

Mögliche Schutzmaßnahmen: Verschlossene Eingrenzungen und Anlagen, elektronische Sperrmechanismen für Protokollierung und detaillierte Autorisierung, Video- und Audioaufzeichnung, PIN- und passwortgesicherte Schlösser, biometrische Authentifizierungssysteme, …(Vgl. ibid)

2.2.2.2 Data Link Layer

Der **Data Link Layer** (*Sicherungsschicht*) bündelt die Bitströme zu Datenpaketen (*frames*) und steuert die Übertragung auf den Übermittlungsabschnitten zwischen den Knoten der Kommunikationsnetze. Diese Schicht ist für die Übertragungsfehlererkennung und -korrektur mithilfe fehlererkennender bzw. fehlerkorrigierender Codes (z.B. Cyclic Redundancy Checks) verantwortlich, definiert darüber hinaus Protokolle zur Regelung des Medienzugangs und reguliert den Nachrichtenfluss zwischen Sender und Empfänger. (Vgl. Eckert 2012:96ff und Schneider 2012:306f)

Dieser Layer war lange ein etwas „vernachlässigter" Bereich zwischen den physischen Aspekten von Layer 1 und dem dominierenden Bereich der Firewall in Layer 3 und 4 (Network und Transport Layer), was natürlich bald ausgenutzt wurde (z.B. *wardriving*). Durch die Interaktion dieses Layers mit verschiedenen Medien und unterschiedlicher Hardware ist er ein kritischer Bestandteil der Netzwerkkompatibilität und daher abhängig von strikten Protokollstandards für die gegenseitige Benutzbarkeit der Systeme. (Vgl. Reed 2003:7)

Schwächen: MAC Address Spoofing; Umgehung des VLANs; Spanning-Tree Fehler, die dazu führen, dass die Layer 2-Umgebung Pakete in Endlosschlaufen übermittelt; Switches können dazu gezwungen werden, Datenpakete an alle VLAN Ports zu übermitteln, anstatt nur an die entsprechenden Ports, wodurch die Datenpakete durch jedes an ein VLAN angeschlossenes Gerät abgefangen werden können. (Vgl. ibid:8)

Mögliche Schutzmaßnahmen: MAC Address Filtering; um die Sicherheit zu gewährleisten, sollten VLANs vermieden werden und die *layers of trust* sollten physikalisch voneinander durch Firewall oder dergleichen getrennt sein. (Vgl. ibid)

2.2.2.3 Network Layer

Der **Network Layer** (*Netzwerkschicht*) wählt den günstigsten Weg für die zu übermittelnden Datenpakete durch die Netze (*routing*), meist über Knoten, stellt Netzadressen für das Internetworking bereit und erkennt und behebt Stausituationen (*congestion control*). (Vgl. Eckert 2012:96ff und Schneider 2012:306f)

Bei den vielen Aufgaben des Network Layers ergeben sich einige Schwächen. So haben die meisten Routingprotokolle nur ein rudimentäres Sicherheitslevel. Identität ist ein klas-

sischer Angriffsvektor und gerade Protokolle für diesen Layer haben oft keine Mittel um die Adressenquelle oder andere Protokolldaten, die für einen Identitätsnachweis genutzt werden können, zu authentifizieren. Die allgegenwärtige Schutzmaßnahme bei Layer 3 ist die Firewall. (Vgl. Reed 2003:9f)

Schwächen: Route spoofing, IP Address Spoofing … (Vgl. ibid)

Mögliche Schutzmaßnahmen: Firewalls mit Filtern und Anti-Spoof Maßnahmen, ARP/Broadcast monitoring software, … (Vgl. ibid)

2.2.2.4 Transport Layer

Der **Transport Layer** (*Transportschicht*) steuert und überwacht medienunabhängig die korrekte Übermittlung der Datenpakete/Nachrichten zwischen den Kommunikationsteilnehmern an den Kommunikationsenden. (Vgl. Eckert 2012:96ff und Schneider 2012:306f)

Dieser Layer ist der erste logische Layer des OSI-Modells. Hier werden mehrere Datenkonversationen von oder zu einem einzelnen Host mithilfe des Multiplexverfahrens gebündelt und auch sortiert. Eine der Schwächen dieses Layers liegt bei der (Wieder- und Über-) Verwendung von Ports für multiple Funktionen, was eine Zugriffseinschränkung durch eine Firewall erschwert. (Vgl. Reed 2003:11f)

Schwächen: fingerprinting, Überverwendung von Ports, spoofing (Vgl. ibid.)

Mögliche Schutzmaßnahmen: Firewall-Regeln, die den Zugriff auf Transmission Protocols und Sub-Protokoll-Informationen (wie TCP Portnummer) einschränken; Stateful Packet Inspection (SPI); bessere Transmission und Layer Session Mechanismen um Angriffe zu vermeiden; … (Vgl. ibid.)

2.2.2.5 Session Layer

Im Gegensatz zu den gerade beschriebenen, kommunikationsorientierten Schichten sind die oberen drei Schichten für datenverarbeitungstypische Aufgaben verantwortlich:

Der **Session Layer** (*Sitzungsschicht*) soll die Kommunikation zwischen Anwendungen gewährleisten und Vorkehrungen für ein Wiederherstellen unterbrochener Sitzungen treffen. Dazu werden Informationen zu sogenannten *checkpoints* (Sicherungspunkten) in den Datenstrom integriert, damit an diesen Punkten die Nachricht oder der Transfer nach einer Unterbrechung wieder aufgenommen werden kann. (Vgl. Eckert 2012:96ff und Schneider 2012:306f)

Schwächen: Schlechte oder keine Authentifizierungsmechanismen; unverschlüsselte Weiterreichung von Session credentials (Abfangen und unautorisierte Verwendung möglich); Session-Identifikation durch spoofing und hijacking gefährdet; … (Vgl. Reed 2003:16)

Mögliche Schutzmaßnahmen: Verschlüsselte/r Passwortaustausch und –speicherung; Verfall von Credentials und Autorisierung; Limitierung von fehlgeschlagenen Sessionversuchen durch Zeitmechanismen (kein Lockout); … (Vgl. ibid.)

2.2.2.6 Presentation Layer

Die Aufgabe des **Presentation Layers** (*Darstellungsschicht*) ist es, die heterogenen Daten der miteinander kommunizierenden Systeme in ein netzeinheitliches Format zu bringen und die Bedeutung der übermittelten Strukturen zu erhalten. Außerdem ist diese Schicht häufig auch für Datenkompression oder Datenverschlüsselung verantwortlich. (Vgl. Eckert 2012:96ff und Schneider 2012:306f)

Schwächen: Schlechte Abwicklung von unerwartetem Input kann zu Applikationsabstürzen führen (Buffer Overflow); Kryptographische Fehler ermöglichen die Umgehung von Datenschutzeinstellungen; … (Vgl. Reed 2003:18)

Mögliche Schutzmaßnahmen: Überprüfung und Spezifikation des Inputs in Applikationen und Bibliotheksfunktionen; sorgfältige und regelmäßige Überprüfung der Verschlüsselungsmöglichkeiten, um die vorhandene Sicherheit mit den bekannten und neu auftauchenden Bedrohungen zu vergleichen; (Vgl. ibid)

2.2.2.7 Application Layer

Der **Application Layer** (*Anwendungsschicht*) stellt Anwendungsdienste bzw. Protokolle bereit, die dem Benutzer zur Verfügung stehen wie SMTP, HTTP, FTP. In dieser Schicht finden sich personenbezogene Absicherungssysteme und Anwendungen zur Abwehr von Schadprogrammen. (Vgl. Eckert 2012:96ff und Schneider 2012:306f)

Schwächen: Programmlogikfehler können dazu benutzt werden, um Programmabstürze oder unerwünschtes Verhalten herbeizuführen; zu komplexe Sicherheitsmechanismen der Applikationen können umgangen werden oder werden schlecht verstanden und umgesetzt; schlechte Schutzmaßnahmen führen zu einem „Alles oder nichts“ – Ansatz (zu viel oder zu wenig Zugriff); (Vgl. Reed 2003:21)

Mögliche Schutzmaßnahmen: Zugriffskontrollen auf Applikationsebene um den Zugriff auf die jeweiligen Applikationsressourcen zu bestimmen; detaillierte und flexible, aber eindeutige Kontrollen; IDS um Applikationsanfragen und –aktivitäten zu beobachten; hostbasierte Firewalls für die Regulierung von Datentransfer je Applikation, wodurch unautorisierte oder versteckte Netzwerkbenutzung verhindert werden kann; (Vgl. ibid)

2.2.3 Rechtliche Grundlagen und Normen

Nicht nur Sicherheitsaspekte sind eine wichtige Grundlage in der IT; auch rechtliche Grundlagen und die vorhandenen Normen spielen eine wichtige Rolle, weshalb einige davon in diesem Kapitel behandelt werden. Da der Autor in einem klinischen Umfeld arbei-

tet, wurde neben der ISO 27001 auch das Medizinproduktegesetz in Bezug auf Software berücksichtigt.

2.2.3.1 ISO 27001

Die nachfolgend behandelte Norm ISO 27001 Information technology – Security techniques – Information security management systems – Requirements „beschreibt die Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS)“ (Müller 2014:58). Durch die umfassende Überarbeitung der Norm im Jahre 2013 sollten nicht nur einheitlichere und klarere Begriffe eingeführt werden, sondern auch klar gestellt werden, dass die Norm ein Management-Standard beschreibt und keinen reinen IT-Security Standard. In der Praxis war es durchaus üblich, den Begriff *Assets* (der eigentlich alle Unternehmenswerte beschreibt) nur mit den IT-Assets einer Organisation gleichzusetzen. Die überarbeitete Norm betont nun klar die Bedeutung von Informationen als *primary assets.* (Vgl. Jendrian 2014)

Ein ISMS wird laut Standard ISO 27001 folgendermaßen definiert:

> *„Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt.*
>
> *ANMERKUNG Das Managementsystem enthält die Struktur, Grundsätze, Planungsaktivitäten, Verantwortung, Praktiken, Verfahren, Prozesse und Ressourcen der Organisation.“*
>
> *(Standard ISO 27001:2013)*

Wie in der Definition klar dargelegt, ist das ISMS nur Teil eines umfassenderen Managementsystems. Kersten et al. (2013) beschreiben in ihrer Literatur die vielfältigen Aufgaben des ISMS sehr übersichtlich und klar:

> *„Es legt fest, welche konkrete Ausprägung der Informationssicherheit benötigt wird (‚die Entwicklung … der Informationssicherheit‘).*
>
> *Es stellt Maßnahmen bereit, die der Informationssicherheit dienen (‚die … Implementierung … der Informationssicherheit‘).*
>
> *Es gibt vor, auf welche Weise Informationssicherheit im täglichen Arbeitsablauf erreicht wird (‚die … Durchführung… der Informationssicherheit‘).*
>
> *Es dient dazu, den erreichten Stand bezüglich der Informationssicherheit sichtbar zu machen und aufrecht zu erhalten (‚die … Überwachung … der Informationssicherheit‘).*

> *Es ermöglicht, den Status der Informationssicherheit nachvollziehbar zu machen („die … Überprüfung … der Informationssicherheit“). Der Unterschied zum vorangehenden Aspekt liegt hier im Soll-Ist-Vergleich, aus dem u. a. der Reifegrad des ISMS erkannt werden kann. Dieser Status ist wichtig, wenn eine Zertifizierung angestrebt wird.*
>
> *Es hilft, den erreichten Stand der Informationssicherheit in Zukunft zu erhalten („die … Instandhaltung … der Informationssicherheit“).*
>
> *Es legt den Grundstein dafür, die Informationssicherheit zu verbessern („die … Verbesserung der Informationssicherheit“).“*
>
> *(Kersten et al. 2013:46f)*

In der ISO 27001:2005 noch explizit erwähnt, folgt auch die überarbeitete Version von 2013 dem PDCA-Zyklus (Plan-Do-Check-Act; oder auch: Planen-Durchführen-Prüfen-Handeln), der nicht nur bei ständigen Verbesserungen des ISMS, sondern auch bei einer Anpassung oder kompletten Neuausrichtung des ISMS, sollten sich die Verhältnisse der Organisation ändern, angewendet werden soll. So lassen sich alle Hauptkapitel der Norm einem der vier Teile des Zyklus zuordnen: Die Kapitel Kontext der Organisation, Führungsrolle, Planung und Unterstützung fallen unter „Plan“, Kapitel Nr. 5 Betrieb kann „Do“ zugeordnet werden, zu „Check“ zählt das Kapitel Leistungsbewertung und das letzte Kapitel Verbesserung gehört zu „Act“. (Vgl. Jendrian 2014, Kersten et al. 2013:47f und Müller 2014:61)

Die folgende Abbildung aus Kersten et al. (2013:48) bietet hierzu noch einen guten Überblick:

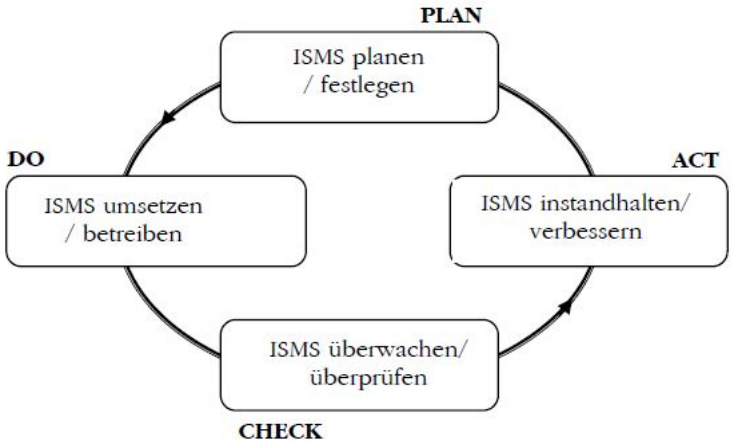

Abbildung 2-3: Der PDCA-Zyklus (Quelle: Kersten et al. 2013:48)

2.2.3.2 Medizinproduktegesetz

Da das berufliche Umfeld des Autors ein klinisches ist, wird in diesem Unterkapitel näher auf das Medizinproduktegesetz eingegangen und dieses zusammengefasst.

Mit dem 1.1.1997 trat das österreichische Medizinproduktegesetz (MPG) in Kraft, die österreichische Medizinproduktebetreiberverordnung folgte am 1.4.2007.

In §1 des MPG wird dessen Anwendungsbereich zusammenfassend dargestellt:

> *„Dieses Bundesgesetz regelt die Funktionstüchtigkeit, Leistungsfähigkeit, Sicherheit und Qualität, die Herstellung, das Inverkehrbringen, den Vertrieb, das Errichten, die Inbetriebnahme, die Instandhaltung, den Betrieb, die Anwendung, die klinische Bewertung und Prüfung, die Überwachung und die Sterilisation, Desinfektion und Reinigung von Medizinprodukten und ihres Zubehörs sowie die Abwehr von Risken [sic!] und das Qualitätsmanagement beim Umgang mit Medizinprodukten und ihrem Zubehör.“ (MPG)*

Nach §2 des österreichischen MPG sind „alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, Software, Stoffe oder anderen Gegenstände, einschließlich der vom Hersteller speziell zur Anwendung für diagnostische oder therapeutische Zwecke bestimmten und für ein einwandfreies Funktionieren des Medizinprodukts eingesetzten Software“ Medizinprodukte, sofern sie zur Anwendung beim Menschen für bestimmte Zwecke (näheres hierzu unter §2 des MPG) bestimmt sind.

Unter Abschnitt 1 des II. Hauptstückes (§§6-12) werden die Anforderungen an Medizinprodukte angeführt. Eine grundlegende Anforderung ist unter anderem, dass Medizinprodukte „so ausgelegt und hergestellt sein [müssen], daß ihre Anwendung weder den klinischen Zustand oder die Sicherheit der Patienten noch die Sicherheit der Anwender oder Dritter gefährdet, wenn sie unter den vorgesehenen Bedingungen und zu den vorgesehenen Zwecken eingesetzt werden.“ (MPG §8 Absatz 1)

In Österreich wird anstelle eines Zulassungsverfahrens eine CE-Zertifizierung des Medizinproduktes gemäß dem MPG oder den entsprechenden EU-Richtlinien gefordert.

Im 1. Abschnitt des V. Hauptstückes (§§80-92) werden das Errichten, Betreiben, Anwenden und Instandhalten von Medizinprodukten in und außerhalb von Einrichtungen des Gesundheitswesens behandelt. Die Medizinproduktebetreiberverordnung (MPBV) gilt ebenfalls für das „Errichten, Betreiben, Anwenden und Instandhalten von Medizinprodukten in Einrichtungen des Gesundheitswesens“ (§1, MPBV) und erweitert die Verordnungen des MPG für bestimmte Arten, Gruppen oder Klassen von Medizinprodukten für Anforderungen, die über die in §80, Absatz 1 definierten hinausgehen.

So haben bei Medizinprodukten beispielsweise Eingangsprüfungen vor deren erstmaliger Verwendung stattzufinden, alle Personen, die das Gerät handhaben, müssen eingewiesen werden und Instandhaltungen müssen so vorgenommen werden, dass keine Person gefährdet wird.

Am 30.12.2009 wurden beide Gesetze nach den Änderungen der EU-Richtlinien 90/385/EWG und 93/42/EWG durch EU-Richtlinie 2007/47/EG novelliert. Unter anderem war bei dieser Änderung auch der Bereich Software betroffen. So wird nun klargestellt, dass „Software als solche, wenn sie spezifisch vom Hersteller für einen oder mehrere der in der Definition von Medizinprodukten genannten medizinischen Zwecke bestimmt ist, ein Medizinprodukt ist“ (Gärtner 2008:20). Somit wird klar, dass auch der IT-Bereich in einer Klinik zunehmend von einzuhaltenden Normen betroffen ist.

Aus dieser kurzen Übersicht ist bereits ersichtlich, dass auch im Bereich der Software im klinischen Umfeld besondere Vorsicht walten zu lassen und auch die Einhaltung von Normen oder Gesetzen sehr wichtig ist.

2.2.3.3 Informationssicherheit in klinischen Unternehmen – Patientendaten

Dem Thema Datenschutz kommt nicht nur im klinischen Bereich ein sehr großer Wert zu; in sämtlichen Unternehmen spielt Datenschutz – ob personen- oder firmenbezogene Daten – eine große Rolle und ist daher ein wichtiger Teil der IT-Compliance („die Befolgung von rechtlichen Pflichten und Geboten im Hinblick auf die in den Unternehmen angesiedelte Informationstechnik“ [Schneider 2012:516]).

Die wichtigste Rechtsvorschrift zum Datenschutz ist in Österreich das Datenschutzgesetz 2000, BGBl I Nr. 165/1999 idgF. (DSG). Das deutsche Pendant dazu ist das Bundesdatenschutzgesetz (BSDG).

In §1 des DSG findet sich die Verfassungsbestimmung (Grundrecht auf Datenschutz):

> *„Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht.“ (DSG)*

Zu diesem Absatz finden sich natürlich auch zahlreiche Ausnahmen, unter anderem selbstverständlich die Zustimmung der betroffenen Person. So wird die Geheimhaltung nicht verletzt, wenn „der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt“ (§9, Z6, DSG)

Auch in Bezug auf Patientendaten findet sich in §9 zu den schutzwürdigen Geheimhaltungsinteressen bei Verwendung sensibler Daten ein Absatz:

> *„Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn […]*
>
> *12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für*

> *die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, […]." (DSG)*

Die gespeicherten Daten eines jeden Patienten sind so also für das behandelnde ärztliche Personal oder Pflegepersonal zugänglich, vor weiterer – missbräuchlicher – Verwendung müssen sie aber geschützt werden. Daher sind gerade dieser Bereich und somit auch der ausreichende Schutz der PCs und ein kontrolliertes Zugriffssystem in einer klinischen Umgebung von großer Wichtigkeit.

2.3 Gefahrenpotential

Jedes IT-System unterliegt grundsätzlich mehr oder weniger allgemeinen Gefahren und Bedrohungen. Je komplexer ein System, desto höher ist auch das Risiko, dem das System unterliegt. Nicht nur die IT-Systeme selbst (Systeme, Daten und Dienste), auch andere Wirtschaftsgüter mit wirtschaftlichem Wert für die Organisation können durch einen Angriff indirekt betroffen sein. Dazu zählen beispielsweise Kalkulationen, Kunden- oder Mitarbeiterinformationen oder auch Forschungs- und Entwicklungsdaten. (Vgl. Pohlmann & Blumberg 2004:44)

Typische Bedrohungen und Szenarien werden in einschlägigen Maßnahmenkatalogen, wie dem IT-Grundschutzkatalog des BSI (Bundesamts für Sicherheit in der Informationstechnik) ausführlich dargestellt. (Vgl. ibid. 43f) Nach einem Überblick über die verschiedenen Gefährdungskategorien nach dem IT-Grundschutzkatalog wird auch noch näher konkret auf die verschiedenen Gefahrenquellen eingegangen.

2.3.1 Gefährdungskategorien nach dem IT-Grundschutz-Katalog (BSI, Deutschland)

Der IT-Grundschutzkatalog verfolgt ein grundlegendes Ziel: „einen angemessenen Schutz für alle Informationen einer Institution zu erreichen" (IT-Grundschutz 1). Dabei spielt der ganzheitliche Ansatz, also eine Kombination aus organisatorischen, personellen, infrastrukturellen und technischen Standardsicherheitsmaßnahmen eine wichtige Rolle, um ein angemessenes und ausreichendes Sicherheitsniveau zu erreichen. (Vgl. ibid)

Die Gefährdungskataloge des IT-Grundschutzes werden in 5 Kategorien (G 1 – G 5) unterteilt; zusätzlich wurde noch eine sechste Kategorie (G 0) eingeführt, die verallgemeinerte und auf das wesentlich reduzierte Gefährdungen beschreibt und hilfreich für Risikoanalysen ist. Für die nachfolgende Analyse der Gefährdungskategorien wurde zusätzlich zum IT-Grundschutz-Katalog auch Pohlmann & Blumberg 2004 (44ff) herangezogen.

Die grundlegenden Ursachen von Gefahren für Kommunikationssysteme, IT-Dienste oder IT-Systeme lassen sich auf Naturereignisse, Ausfall von Technik oder Fehlhandlungen von

Menschen festlegen. Die folgenden Kategorien des IT-Grundschutzkatalogs führen dies näher aus:

G 0: Elementare Gefährdungen

Wie oben erwähnt, beschreibt G 0 verallgemeinerte Gefährdungen, die auf das Wesentliche reduziert werden; dazu zählen beispielsweise Feuer, Wasser oder elektromagnetische Störstrahlung.

G 1: Höhere Gewalt

Höhere Gewalt, oder auch Force Majeure, sind Ereignisse, die außerhalb des Einflusses der betroffenen Personen oder Parteien stehen, wie Naturkatastrophen (Erdbeben, Hochwasser, Sturm), Kriege oder terroristische Handlungen.

G 2: Organisatorische Mängel

Unter der Kategorie organisatorische Mängel werden Gefährdungen zusammengefasst, die durch schlechte Planung in den Bereichen betriebswirtschaftliche Abläufe/Prozesse, Berichtsstrukturen oder Verantwortungsbereiche entstehen. Dazu zählen unter anderem unzureichende Kontrolle der Sicherheitsmaßnahmen, unbefugter Zutritt, unzureichend geschützte Verteiler oder auch ungeregelte Weitergabe von Datenträgern.

G 3: Menschliche Fehlhandlungen

Unter menschlichen Fehlhandlungen versteht das BSI in Kategorie G 3 nur unwissentliche Fehlhandlungen wie fehlerhafte Nutzung oder Administration von IT-Systemen, unbeabsichtigtes Löschen von Daten oder Programmen oder Sorglosigkeit im Umgang mit Informationen.

G 4: Technisches Versagen

Technisches Versagen von sowohl Hard- als auch Software kann verschiedenste Ursachen wie komplexe Schutzsysteme, Überlastung durch fehlendes Knowhow der Mitarbeiter oder Ähnliches haben. Katalog G 4 subsummiert solches Fehlverhalten: darunter fallen beispielsweise Ausfall von Stromversorgung oder Sicherheitseinrichtungen, defekte Datenträger, Störungen von Kommunikationswegen, oder auch der Ausfall von Systemen von externen Dienstleistern.

G 5: Vorsätzliche Handlungen

Die Kategorie vorsätzliche Handlungen beschreibt das wissentliche Fehlverhalten von Personen, die berechtigter- oder unberechtigterweise Zugriff auf IT-Systeme oder Dienste erhalten. Dazu zählen Manipulation von sowohl Geräten als auch Da-

ten, Vandalismus, Missbrauch von Benutzer- oder Administratorrechten oder Sabotage.

Einen guten Überblick über die fünf ursprünglichen Kategorien der Gefährdungskataloge bietet die folgende Abbildung aus Eckert 2012:

Abbildung 2-4: Gefährdungsfaktoren (Quelle: Eckert 2012:17)

2.3.2 Gefahren- und Fehlerquellen

Wie bereits die Gefährdungskategorien des IT-Grundschutzkataloges darlegen, gibt es verschiedenste Arten von Gefahrenquellen (Bedrohungen) oder Fehlerquellen für IT-Systeme und IT-Dienste.

2.3.2.1 Fehlerquellen

Es gibt zahlreiche Fehlerquellen im Bereich der IT; laut Pohlmann & Blumberg (2004:54) zählen neben menschlichem Versagen dazu auch technische Defekte oder höhere Gewalt (die wiederum zu technischen Defekten führen kann), die im Folgenden näher ausgeführt werden (nach Pohlmann & Blumberg 2004:54ff)

Übertragungsfehler

Durch verschiedene Einflüsse (Wackelkontakt, Übersprechen zwischen parallel verlaufenden Leitungen etc.) ist es möglich, dass einzelne Bits einer Übertragung verfälscht werden.

Softwarefehler

Da letztlich jede Software vom Menschen erstellt wird, hängt deren Qualität in starkem Maße von der Kompetenz des verantwortlichen Programmierers und seinen Rahmenbedingungen ab, weswegen Qualitätssicherung ein wichtiger Teil jeder Softwareentwicklung darstellen sollte. Die steigende Komplexität von Programmen und der wachsende Zeitdruck auf Programmierer in der heutigen Zeit sind zwei schwerwiegende Ursachen für Programmierfehler. Gerade durch den Zeitdruck werden auf Komponenten der Entwicklung verzichtet, die auch für die Qualitätssicherung unumgänglich sind, wie die lückenlose Dokumentation und im nächsten Schritt hinreichende Tests oder Testszenarien. Aufgrund der oft sehr komplexen Softwarepakete sind jedoch vollständige Tests mit allen möglichen Konstellationen meist nicht durchführbar. Dies führt dazu, dass im Prinzip davon ausgegangen werden muss, dass die verwendete Software nicht komplett fehlerfrei ist und daher mit Fehlfunktionen zu rechnen sind. Gerade in Institutionen wie Kliniken können solche Fehlfunktionen auch durchaus gefährliche Folgen haben.

Hardwarefehler

Im Gegensatz zu einer Software, die ständig weiterentwickelt werden kann, hat Hardware eine begrenzte Lebensdauer. Die Anfälligkeit für Fehler ist dabei besonders am Anfang („Kinderkrankheiten“) und gegen Ende der Nutzungsdauer groß. Hardwareausfälle können beispielsweise durch eine Beeinflussung der Betriebstemperatur (Überspannung, Stromausfälle, extreme Temperaturschwankungen etc.) oder Feuchtigkeit beschleunigt werden.

Umwelteinflüsse

IT-Systeme können durch unterschiedliche Umweltfaktoren beeinflusst werden: Funkübertragungen können durch kosmische und solare Strahlung gestört werden, Blitzschläge rufen Überspannungen auf den Kommunikations- und Versorgungsnetzen hervor.

Bedienfehler

Schlussendlich stellt auch „menschliches Versagen“ eine Fehlerquelle dar. Durch Unkenntnis, unzureichende Konzentration oder auch fehlende Sensibilisierung für die notwendige Sicherheit eines IT-Systems des Mitarbeiters können Fehler passieren, die man anderenfalls hätte vermeiden können. Durch Schulungen oder Erstel-

len von SOPs (Standard Operating Procedures), die die Mitarbeiter befolgen können, ist es möglich, solche Bedienfehler zu minimieren.

2.3.2.2 Angriffe

Ein Angriff – ein nicht autorisierter Zugriff bzw. Zugriffsversuch auf ein System – ist eine aktive Bedrohung für ein IT-System, die erst durch dessen Nutzung möglich wird. Es können zwei grundlegende Angriffsarten unterschieden werden: *aktive* und *passive* Angriffe. (Vgl. Pohlmann & Blumberg 2004:46 und Eckert 2012:19)

Passive Angriffe

Passive Angriffe haben die unautorisierte Informationsgewinnung („Abhören“) zum Ziel und haben deshalb den Verlust der Vertraulichkeit zur Folge (vgl. Eckert ibid.). Beim passiven Angriff wird der Betrieb vom betroffenen IT-System vom Angreifer nicht gestört, bzw. nicht merkbar beeinflusst oder modifiziert. Je nach Art der Kommunikationssysteme unterscheidet sich auch der Aufwand für den Angreifer. Bei der Nutzung eines ungesicherten oder schlecht gesicherten WLANs oder von modifizierter Software, die die Datenströme kopiert, hat der Angreifer beispielsweise ein relativ leichtes Spiel. Oft handelt es sich bei der Information, die der Angreifer wünscht, um Zugangsdaten für gesicherte Systeme, wie Banksysteme oder Datenbanken, was ihm dann im weiteren Verlauf einen aktiven Angriff erlaubt. (Vgl. Pohlmann & Blumberg 2004:47f)

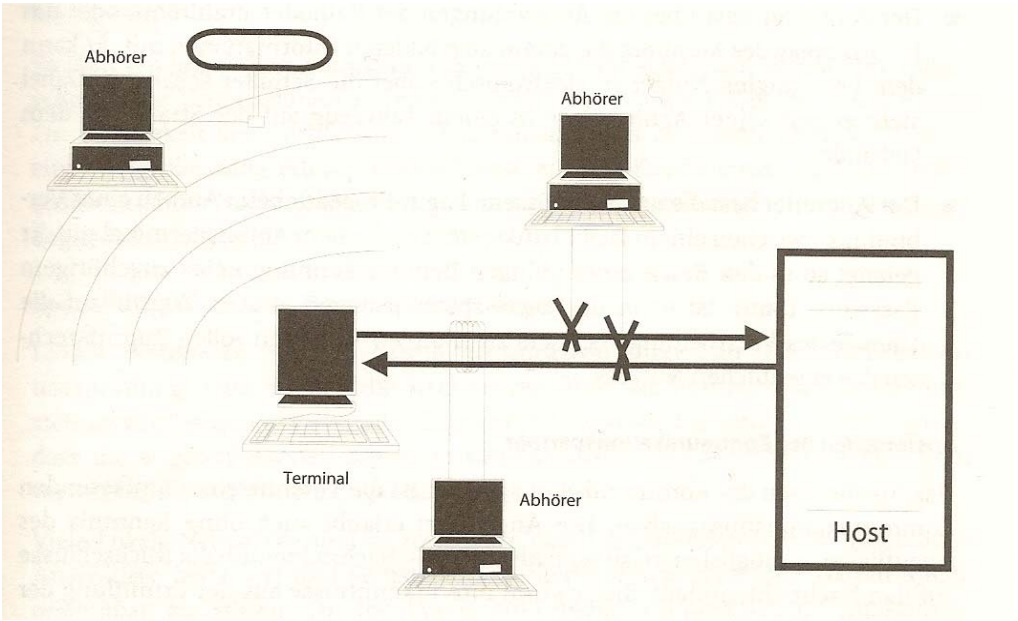

Abbildung 2-5: Abhören von Informationen (Quelle: Pohlmann & Blumberg 2004:45)

Aktive Angriffe

Bei einem aktiven Angriff wird im Gegensatz zu einem passiven Angriff der Datenstrom manipuliert oder auch die Erreichbarkeit eines Systems beeinflusst. Der

Angreifer greift direkt ein und verfälscht oder modifiziert die zu übermittelnden Daten. Ein aktiver Angriff beeinträchtigt somit die Datenintegrität und/oder Verfügbarkeit eines IT-Systems. (Vgl. Eckert 2012:19 und Pohlmann & Blumberg 2004:50f) Wie in nachfolgender Abbildung gut zu erkennen, „sitzt" der Angreifer zwischen den Beteiligten („Man-in-the-middle"), von wo aus er aktiv eingreifen kann.

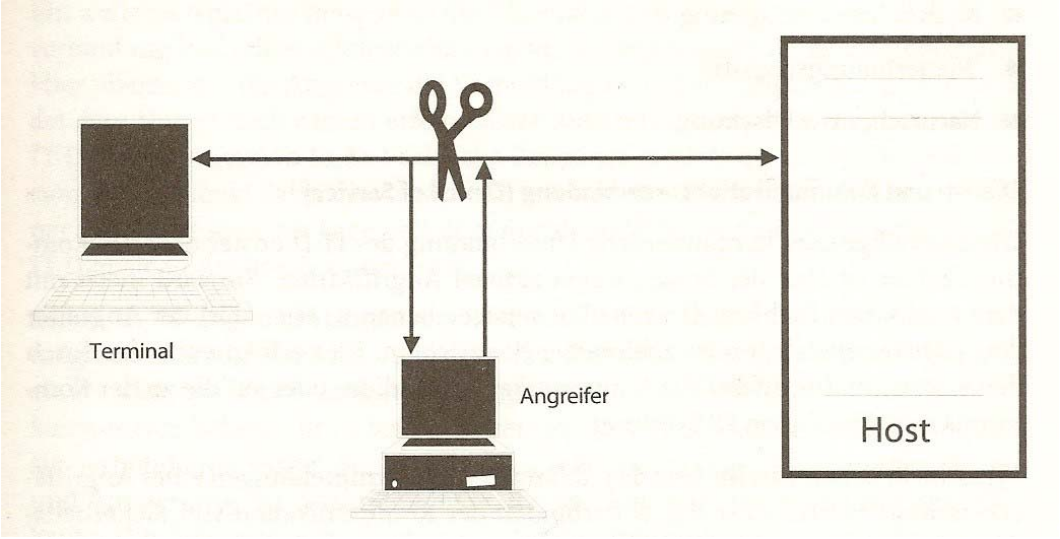

Abbildung 2-6: Aktiver Angriff (Quelle: Pohlmann & Blumberg 2004:49)

Im Nachfolgenden sollen noch einige der typischen aktiven Angriffe definiert werden.

Bei Angriffen, deren Ziel es ist, die Verfügbarkeit (*availability*) eines IT-Dienstes oder IT-Komponenten zu stören oder zu unterbinden, spricht man von *denial of service*. Diese bekannte Angriffsart erzielt die Störung des Dienstes, indem dessen Kommunikationswege durch zahllose Nachrichten, Verbindungsversuche etc. überschwemmt werden. (Vgl. Eckert 2012:19 und Pohlmann & Blumberg 2004:52) DDoS-Attacken haben vergleichsweise noch eine höhere Wirkung, da hier mehrere Computer gleichzeitig einen Dienst angreifen, um z.B. die Internetanbindung, die Ressourcen der Netzwerkkomponenten oder die Web- und Datenbankserver zu überlasten. (Vgl. CERT 2017)

Die Angriffsart *Nachrichtenverzögerung* setzt es sich zum Ziel, die Zustellung von Nachrichten gezielt zu verzögern. Bei zeitkritischen Systemen (z.B. einem Echtzeitsystem) kann eine Hemmung der Nachrichtenübermittlung bis hin zur vollständigen Blockade fatale Folgen haben. (Vgl. Pohlmann & Blumberg 2004:52) Bei einem autonom fahrenden Vehikel kann beispielsweise verzögertes Bremsen (durch Hemmung der Nachrichtenübermittlung) trotz „Gefahr erkannt" fatal enden.

Der *Wiederholungsangriff* sendet eine bereits übermittelte Nachricht erneut oder mehrmals. Bei einer mehrfachen Übermittlung eines Überweisungsauftrages kann

so zum Beispiel die mehrfache Durchführung erwirkt werden. (Vgl. Pohlmann & Blumberg 2004:52)

Bei der Angriffsart *Nachrichtenverfälschung* wird vom Angreifer der Dateninhalt einer Nachricht verändert oder manipuliert. Beim bereits erwähnten Überweisungsauftrag können so Kontodaten und Betrag geändert werden. Außerdem möglich ist das sogenannte *session-highjacking*, bei dem der Angreifer die Verbindung eines berechtigten Nutzers nach dessen Login übernimmt und somit den jeweiligen IT-Dienst mit den Rechten des eigentlichen Nutzers in Anspruch nehmen kann. (Vgl. Pohlmann & Blumberg 2004:53)

Eine in den letzten Jahren immer häufigere Angriffsart ist das sogenannte *Phishing*, das sich gerade in Bereichen wie Internet Banking „etabliert" hat. Beim Phishing werden den Opfern verlockende Angebote gemacht oder sie werden um Hilfe gebeten, um an deren Zugangsdaten zu kommen oder auch Geldzahlungen zu erhalten. (Vgl. Schneider 2012:395)

2.3.2.3 Schadsoftware

Bei der Entstehung neuer Technologien und Kommunikationssysteme lassen auch meist böswillige Angriffe und Schadtechnologie nicht lange auf sich warten. Auch bei der Entwicklung der Computertechnologie und der Ausbreitung des Internets war dies nicht anders. Durch die globale Natur der heutigen Technologie und der Abhängigkeit einer modernen Volkswirtschaft von Computern und einer Anbindung an das Internet sind gerade böswillige Angriffe und Schadsoftware (Programme, die nicht erwünscht sind, und vorsätzlich dem Benutzer oder System Schaden zuführen wollen [Vgl. Kappes 2007:93]) zu einer hohen Gefahr geworden. (Vgl. auch Schneider 2012:393)

Viren

Mit der Verbreitung des PCs ging auch die Entstehung von Computerviren einher. Ein Virus benötigt ein Wirtsprogramm für die Ausführung und ist in der Regel ein einfaches Schadprogramm, das nicht nur Programme oder Dateien angreift, sondern auch Rechner. Es reproduziert sich selbst, indem es bei der Ausführung eine „Reproduktion" (oder auch modifizierte Version) in einen Speicherbereich kopiert und somit infiziert – mit dem Zweck andere Soft- und Hardware zu schädigen, oder auch zu zerstören. Mögliche Speicherbereiche, in die sich ein Virus kopieren kann, sind beispielsweise Programmcodes oder Bereiche des Betriebssystems. Wann der Virus seinen Schaden tatsächlich ausführt, kann durch Randbedingungen – wie ein Datum – bestimmt werden. Es können verschiedene Typen von Viren unterschieden werden: Computervirus, Programmvirus, Bootvirus, Skriptvirus, Systemvirus, Dateivirus. Viren können mittels Virenscanner entdeckt werden, aber auch das gestaltet sich angesichts der Vielfalt der ständig neu auftretenden Viren (unter anderem metamorphe Viren oder auch Viren mit „Tarnfunktion") und der Einschrän-

kung bei Blacklisting immer schwieriger. (Vgl. Eckert 2012:55ff und ITWissen, s.v. Virus)

Würmer

Ein Wurm benötigt im Gegensatz zu einem Virus kein Wirtsprogramm, da es ein autonomes Programm darstellt. Es vervielfältigt sich selbständig über Netzwerke um möglichst viele Rechner zu infizieren. Hierbei benötigen sie üblicherweise viele Ressourcen; bei einem eventuellen Mehrfachbefall können die Speicher eines Rechners durch die Würmer ausgeschöpft werden. (Vgl. Eckert 2012:67f und ITWissen, s.v. Wurm)

Trojaner

Ein Trojaner, oder auch trojanisches Pferd, ist ein Schadprogramm, das neben seiner eigentlichen Funktion noch weitere versteckte Funktionen besitzt (analog zum Trojanischen Pferd aus der griechischen Mythologie), die es selbständig im Hintergrund ausführt. Mithilfe dieser verborgenen Funktionen ist es dem Trojaner beispielsweise möglich, Daten aufzuzeichnen oder Systemkonfigurationen zu modifizieren, während dem Benutzer das erwartete Verhalten vorgetäuscht wird. So können die befallenen Rechner kontrolliert werden, Tastatureingaben (wie Passwörter) aufgezeichnet und versendet werden, oder automatisch Updates und weitere Malware heruntergeladen werden. Aktiviert werden die Trojaner meist entweder durch den Programmstart oder auch durch eine *logische Bombe* (Aktivierung durch das Vorhandensein einer bestimmten Bedingung.). (Vgl. Eckert 2012:73f, Schneider 2012:393, ITWissen, s.v. Trojaner)

Trapdoor/Backdoor

Eine Trapdoor, oder auch Hintertür, bezeichnet einen Teil einer Software, mit Hilfe dessen es jemandem ermöglicht wird, auf ein Programm oder ein System ohne Kenntnis oder Nutzung der normalen Zugangssicherung zuzugreifen. Eine solche Trapdoor kann beispielsweise durch ein trojanisches Pferd auf einem Computer installiert werden. (Vgl. Pfleeger & Pfleeger 2007:116)

Rabbit

Ein Rabbit-Programm ist ein Programm, das nur darauf ausgerichtet ist, unlimitiert Kopien seiner selbst zu starten. Das Ziel des Programmes ist es, Computerressourcen zu verbrauchen und somit das System zu blockieren. (Vgl. Pfleeger & Pfleeger 2007:116)

Die folgende Tabelle (aus Pfleeger & Pfleeger 2007) soll noch einmal einen kurzen Überblick über die Typen von Schadsoftware bieten:

Tabelle 2-1: Arten von Schadsoftware (Quelle: Pfleeger & Pfleeger 2007:117)

Code Type	Characteristics
Virus	Attaches itself to program and propagates copies of itself to other programs
Trojan horse	Contains unexpected, additional functionality
Logic bomb	Triggers action when condition occurs
Time bomb	Triggers action when specified time occurs
Trapdoor	Allows unauthorized access to functionality
Worm	Propagates copies of itself through a network
Rabbit	Replicates itself without limit to exhaust resources

Je nach Art des angerichteten Schadens können andere Unterteilungsmöglichkeiten genutzt werden.

Spyware

Mithilfe von Spyware können vertrauliche Informationen (z.B. Zugangsdaten) ohne Wissen des Benutzers weitergeleitet werden. Unter diese Art fallen beispielsweise Keylogger, die die Eingaben durch Maus und Tastatur aufzeichnen und weiterleiten. (Vgl. Kappes 2007:93)

Adware

Adware zeigt dem Benutzer ungewollte Werbung (vgl. Kappes 2007:93). Dabei sind diese Programme meist sehr hartnäckig, wenn versucht wird, sie aus dem System zu entfernen.

Zombie-Malware

Durch dieses Programm wird der Computer „übernommen“ und so zu einem „Zombie“. Das System kann von einem Dritten kontrolliert und gesteuert werden. (Vgl. Kappes 2007:93)

Ransomware

Eine neue Unterform der Bedrohung stellt die sogenannte *Ransomware*, oder auch *Erpressungstrojaner* dar. Hier werden durch einen Trojaner (z.B. *Locky* im Jahre 2016) Dateien verschlüsselt bzw. wird der Zugriff auf sie verhindert. Der Zugriff kann nur durch Bezahlung eines „Lösegeldes“ zurückerlangt werden. Und obwohl Sicherheitsbehörden von der Zahlung dieses Lösegeldes abraten, waren schon viele Unternehmen gezwungen zu zahlen, um den Zugriff auf ihre Daten zurückerlangen.

2.3.2.4 Aktuelle Lage

Wie der Security Report 2015/2016 des AV-Test Institutes (The Independent IT-Security Institute) in Deutschland beweist, ist das Betriebssystem Windows nach wie vor Hauptangriffsziel von jeglicher Art von Malware. Seit Beginn der Messungen durch das Institut 1984 ist die Anzahl der bekannten Windows-Schadprogramme auf über 570 Millionen gestiegen, und für 2016 wurde prognostiziert, dass die 600 Millionen-Grenze überschritten wird.

Abbildung 2-7: Gesamtentwicklung Schadprogramme für Windows seit 2005 (Quelle: AV-Test 2016)

In den letzten zwei Jahren hat sich die Art der verwendeten Schadprogramme jedoch gewandelt. Währen 2015 noch Würmer die beliebteste Art waren – gefolgt von Viren und Trojanern –, so sind 2016 Viren und Trojaner auf dem Vormarsch.

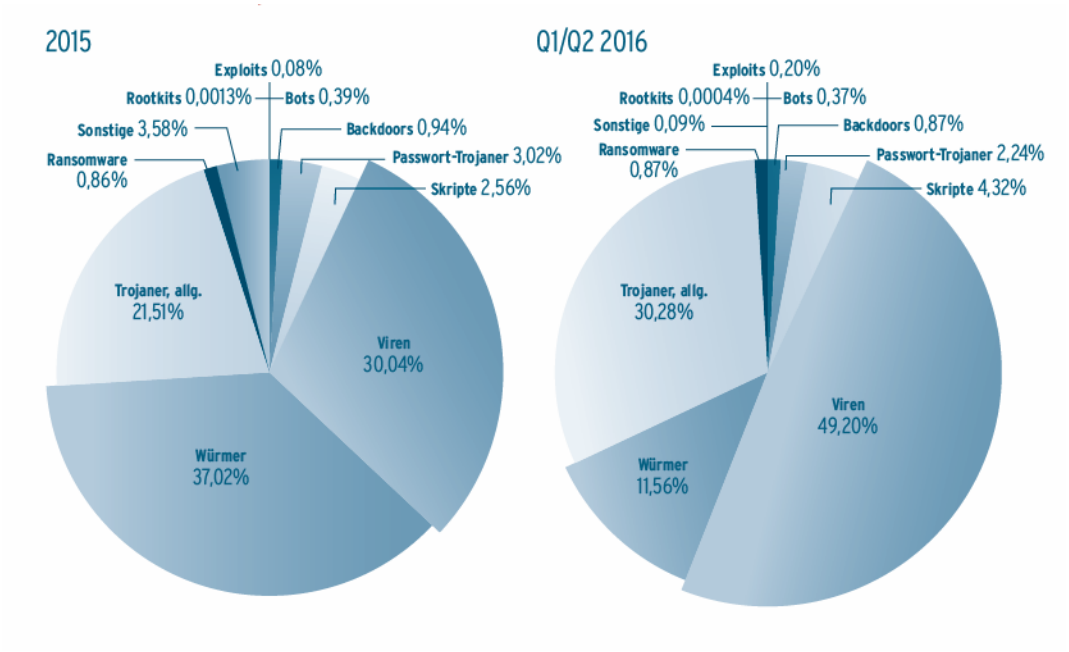

Abbildung 2-8: Malware-Verteilung unter Windows (Quelle: AV-Test 2016)

Ende 2016 wurde bei GUS-Banken eine neuartige Malware entdeckt. Diese nahezu unsichtbaren Attacken werden mithilfe legitimer Software (z.B. weitverbreitete Tools für Penetrationstests und Administratoren, das Power Shell-Framework für Aufgabenautomatisierung unter Windows) durchgeführt und hinterlassen keine Malware-Dateien auf der Festplatte, da sie nur kurzzeitig im Speicher versteckt werden, wo sie unbemerkt Passwörter von Systemadministratoren sammeln. Kaspersky Lab hat seither eine Vielzahl solcher Attacken – verteilt über mehr als 140 Unternehmensnetzwerken in über 40 Ländern – entdeckt. Whitelisting-Technologien sind für die Ausforschung dieser Malware nicht hilfreich; außerdem hinterlässt sie kaum Spuren oder Muster für eine Analyse, nach einem Systemneustart ist nichts mehr zu finden. (Vgl. Pressemitteilung Kaspersky Lab 2017)

> *„Die Entschlossenheit der Angreifer, ihre Aktivitäten zu verstecken und so die Entdeckung und eine Incident Response extrem zu erschweren, zeigt den neuesten Trend antiforensischer Techniken und speicherbasierter Malware […] Speicherforensik wird deshalb für die Analyse von Malware und deren Funktionen besonders wichtig. Bei diesen Attacken nutzten die Angreifer jede denkbare antiforensische Technik und demonstrierten, dass keine Malware-Dateien für das erfolgreiche Herausfiltern von Daten aus einem Netzwerk benötigt werden. Gleichzeitig zeigt sich, dass die Verwendung legitimer und Open-Source-basierter Werkzeuge eine Zuweisung der Attacke fast unmöglich macht.“ (Sergey Golovanov; Pressemitteilung Kaspersky Lab 2017)*

Eine der momentan am häufigsten eingesetzten Attacken – und eine der effizientesten – sind DoS- und DDoS-Attacken, die meist in den Bereichen der Industrie und des Finanzwesens, inzwischen aber auch bei Cyber-Spionage zum Zug kommen (vgl. CERT 2017).

Die letzten Berichte von Kaspersky zu den DDoS-Attacken im dritten und vierten Quartal 2016 (vgl. Khalimonenko et al 2017 und Khalimonenko et al 2016) zeigen, dass letztes Jahr die DDoS-Attacken ein noch nie dagewesenes Ausmaß angenommen haben. Mithilfe von IoT-Botnets, bestehend aus zehntausenden Geräten wie Webcams, Routern und Thermostaten, gab es massive Angriffe gegen beispielsweise den französischen Telekommunikationsanbieter OVH (mit einem Wert von fast 1TB/s) oder auch die Deutsche Telekom. Für viele dieser Angriffe machen Sicherheitsexperten den „Mirai"-Quellcode, der einen integrierten Scanner für die Suche nach verwundbaren IoT-Geräten enthält und diese an ein Botnet anschließt, verantwortlich. Nicht nur Unternehmen sind von solchen Attacken betroffen; DDoS-Attacken werden auch zunehmend für politische Zwecke genutzt.

Europol klassifiziert sowohl Ransomware (im Bereich Malware) als auch DDoS-Attacken (Datenlecks und Netzwerkattacken) als momentane Schlüsselbedrohungen in ihrem Internet Organised Crime Threath Assessment für 2016 (vgl. IOCTA) und für Kaspersky Lab zeigen die vergangenen Angriffe „dass die DDoS-Landschaft im Jahr 2016 mit neuen Technologien, wuchtiger Angriffsstärke sowie hoch qualifizierten und professionellen Cyberkriminellen die nächste Entwicklungsstufe erreicht hat" (Khalimonenko et al 2017). Sie erwarten für 2017 neue Mirai-Botnetz-Modifikationen und eine grundsätzliche Zunahme von IoT-Botnetzaktivität.

Dies stellt nur ein Ausschnitt der sich immer weiter entwickelnden Schadprogramme und Attacken dar.

2.3.2.5 Bedrohungen durch die Endsysteme

Nicht nur die zentralen IT-Systeme, auch die Endsysteme, die Clients, erfreuen sich bei den Angreifern großer Beliebtheit. Oft stellen die Clients aufgrund ihrer Ansammlung diverser Anwendungen einen großen sicherheitstechnischen Aufwand für die betreuenden IT-Administratoren dar. Der Angreifer kann einen erfolgreichen Angriff auf einen Client als Sprungbrett für seinen Angriff auf das zentrale IT-System nutzen. (Vgl. Pohlmann & Blumberg 2004:57)

2.4 Allgemeine/grundsätzliche Sicherheitslösungen

Es gibt unterschiedlichste Sicherheitslösungen, die für Client-Security eingesetzt und miteinander kombiniert werden können. Viele der Sicherheitslösungen können aber auch auf anderen Ebenen (Server etc.) eingesetzt werden.

Antimalwareprogramme/Blacklisting

Antimalwareprogramme (Blacklisting) überprüfen den Rechner auf einen möglichen Malwarebefall aufgrund einer *Blacklist*. Die wichtigsten Funktionen dieser Programme sind (1) die Überprüfung des Systems auf vorhandene Malware, wobei sowohl Speicher als auch einzelne oder alle Laufwerke gecheckt werden; (2) die Überprüfung von Dateien auf Befall bevor diese geöffnet oder ausgeführt werden und bei entsprechender Erkennung bzw. Ver-

dacht wird die Aktion verhindert; und (3) die Entfernung von Malware aus den infizierten Dateien. Das Erkennen von Malware in Dateien ist sehr komplex und nimmt daher viel Zeit in Anspruch. Die Scanner untersuchen die Dateien auf Muster und vergleichen diese mit bekannten Mustern aus der lokalen Datenbank (Blacklist). Da das Programm diese *Signaturen* (Muster) mit einer lokalen Datenbank abgleicht, muss diese ständig aktualisiert werden, um Malware erkennen zu können. (Vgl. Kappes 2007:99) Um auch Malware ohne bekannte Signatur finden zu können, verwenden Malwareprogramme sogenannte *Heuristiken*. Hier wird anhand von bestimmten Regeln bzw. Algorithmen nach verdächtigen Codes gesucht, die einen böswilligen Zweck haben könnten. Modernere Scanner verwenden zudem noch eine *Sandbox* (meist virtuell), womit sie Programme in einer gesicherten Umgebung ausführen können. Die Sandbox ist vom eigentlichen Hostsystem komplett abgeschottet, wodurch die ausgeführten Programme dort ohne Gefahr für das Hauptsystem auf deren Verhaltensweisen überprüft werden können. Im Gegensatz zu heuristischen Methoden kann beim Sandboxing im Detail analysiert werden, was diese Datei genau macht, benötigt aber natürlich mehr Zeit. (Vgl. Cade 2015)

Whitelisting

Im Gegensatz zu Blacklisting wird bei Whitelisting eine Liste oder Inventory erstellt, die die ausführbaren Dateien enthält, die zur Ausführung erlaubt sind. Früher, als die Anzahl der Viren bzw. Malware noch überschaubar war, war Blacklisting die klare Lösung; durch die zunehmende Anzahl an Malware wird es jedoch einfacher, eine Whitelist zu erstellen. Dies ist allerdings auch nur bedingt richtig, da in komplexen Umgebungen die Erstellung einer Whitelist teilweise zu aufwändig wird (z.B. oft Neuinstallation von Programmen). (Vgl. Best Practices 7)

Auf Whitelisting wird in Kapitel 4 noch näher eingegangen, weswegen hier auf eine ausführlichere Erläuterung verzichtet wird.

Updates

Um die Sicherheit eines Systems zu gewährleisten, ist es außerdem wichtig, das System und die darauf installierten Programme immer auf dem aktuellsten Stand zu halten. Dadurch werden Sicherheitslücken, die unter anderem durch Programmierfehler in Betriebssystemen, Browser oder anderen Softwareanwendungen entstehen können und die als Schwachstellen von Malware und Hackern ausgenutzt werden können, geschlossen und es wird für die Malware/Angreifer schwerer das System zu befallen. Je schneller dabei diese Lücken durch Patches geschlossen werden, umso besser: Angreifer schauen sehr genau, welche Sicherheitslücken bekannt werden und richten ihre Schadsoftware direkt auf diese Lücke aus. Daher ist die Benutzung von EOL-Betriebssystemen insofern gefährlich, als es bekannte Sicherheitslücken gibt, die jedoch nicht mehr gewartet werden.

Als Beispiel dafür, wie häufig Sicherheitslücken auch bei aktuellen, ständig gewarteten Betriebssystemen sind, sei hier Windows 10 genannt. Laut der Schwachstellen-Datenbank

„CVE Details“ wurden bisher schon 225 Sicherheitslücken – 172 davon allein im Jahre 2016 – gezählt, wobei die Dunkelziffer natürlich höher sein dürfte (vgl. Eikenberg & Schulz 2017).

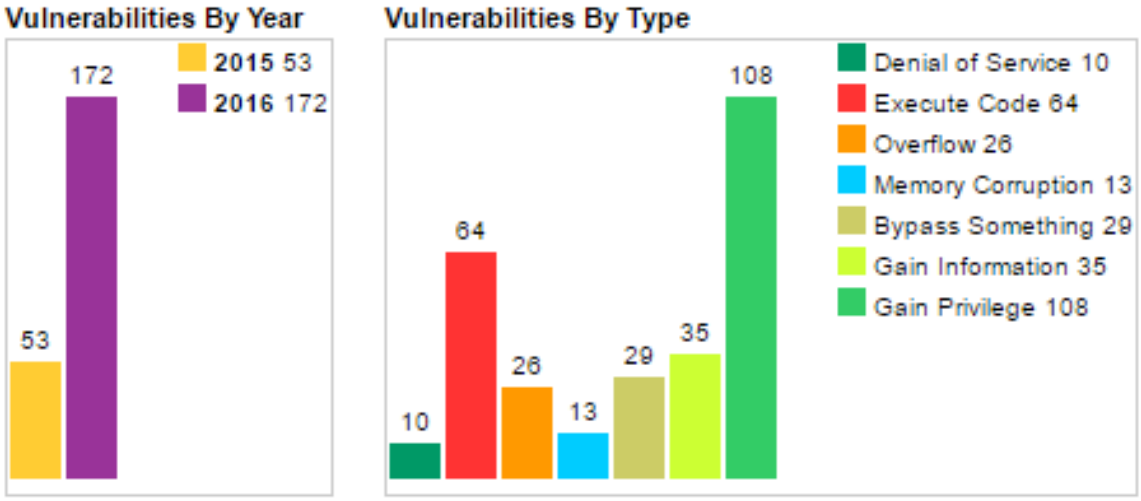

Abbildung 2-9: Sicherheitslücken in Windows 10 nach Jahr und Typ (Quelle: CVE 2016)

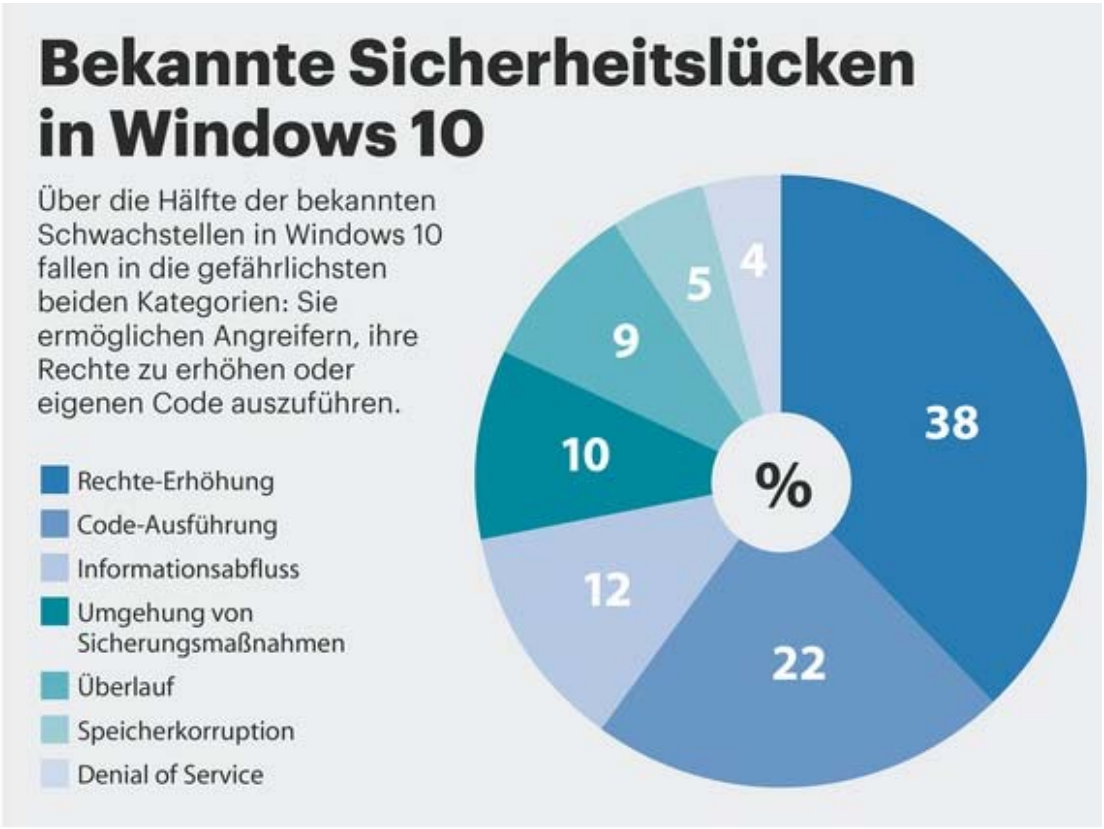

Abbildung 2-10: Sicherheitslücken in Windows 10 in Prozent (Quelle: CVE 2016, zit. n. Eikenberg & Schulz 2017)

Besonders wichtig ist es auch, die benutzte Antiviren-Software aktuell zu halten. Vor allem regelmäßige (tägliche) Datenbankupdates der Virendefinitionen sind diesbezüglich unerlässlich.

Firewall

Ein Firewall-System dient als Schutz vor Gefahren aus unsicheren Netzen und soll die Sicherheitsniveaus der über sie verbundenen Netzwerke trennen. (Vgl. Pohlmann & Blumberg 2004:296)

Eine Firewall hat zwei große Hauptaufgaben: (1) als *Brandschutzmauer* und (2) als *Pförtner*. Die Brandschutzmauer sichert das zu schützende Netz vor einem anderen, unsicheren Netz (wie dem Internet), der Pförtner kontrolliert und protokolliert den Zugang zum zu schützenden Netz. Datenverkehr zwischen den Netzen ist also nur über einen einzigen Weg (die Firewall) möglich. Dieses System stellt somit den *Common Point of Trust* dar. Eine Firewall bietet zahlreiche Vorteile, wie unter anderem die Möglichkeit die Sicherheitspolitik zentral umzusetzen, was auch effizienter ist, als jeden einzelnen Rechner zu schützen. (Vgl. Techstories, s.v. Firewall-Systeme)

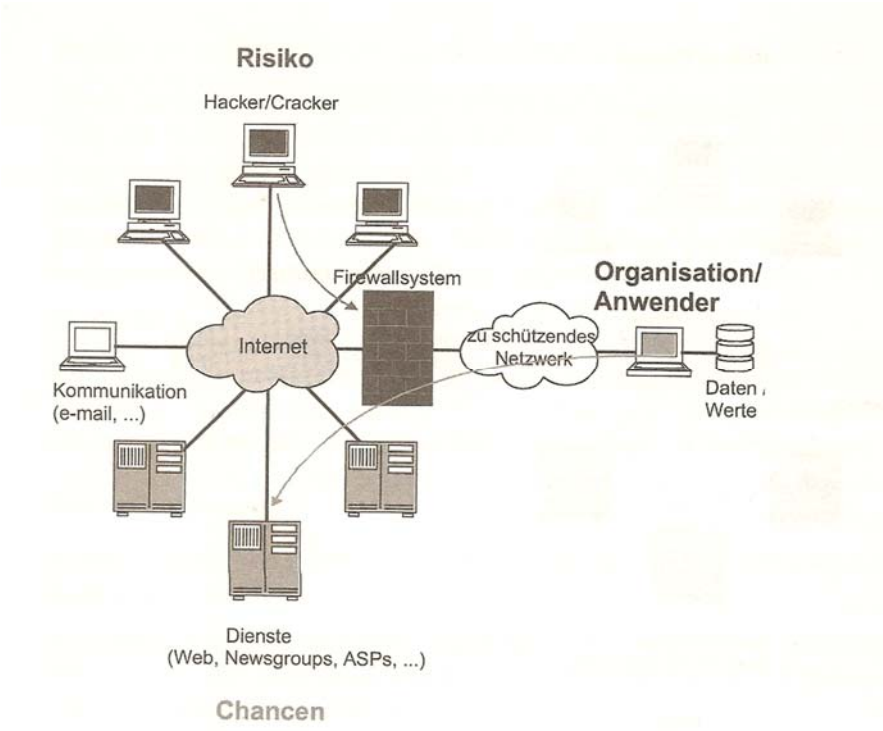

Abbildung 2-11: Firewallsystem (Quelle: Pohlmann & Blumberg 2004:297)

Ein Firewall-System verfolgt die folgenden allgemeinen Ziele:

- *„Zugangskontrolle auf Netzwerkebene: Welche Rechner dürfen miteinander kommunizieren*
- *Zugangskontrolle auf Benutzerebene: Welche Benutzer dürfen über die Firewall eine Kommunikation aufbauen*

- *Zugangskontrolle auf Datenebene: Welche Daten dürfen übertragen werden*
- *Rechteverwaltung: Firewall-Regeln, welche Protokolle und Dienste sind erlaubt*
- *Kontrolle auf Anwendungsebene: Welche Kommandos und Daten sind für die zu schützende Anwendung erlaubt (z.B. SMTP-Proxy, bestimmte gefährliche Befehle sperren)*
- *Entkopplung von Diensten: Kein [sic!] direkte Kommunikation mit den Diensten, damit Implementierungsfehler der Dienste nicht angegriffen werden können (Proxy)*
- *Beweissicherung und Protokollauswertung: Logging*
- *Alarmierung: Über besonders sicherheitsrelevante Ereignisse direkt informieren*
- *Verbergen von internen Netzstruktur: Struktur des zu schützenden Netzes gegenüber unsicheren Netz verbergen (Wie viele Rechner sind angebunden? Welche Betriebssysteme? usw.)*
- *Vetraulichkeit [sic!] der Nachrichten: Durch Verschlüsselung können Nachrichten nicht im Klartext gelesen werden*“ *(Techstories, s.v. Firewall-Systeme)*

Personal Firewall

Eine Personal Firewall (oder auch Desktop Firewall) ist im Gegensatz zum Firewall-System eine Softwarelösung, die auf dem Endgerät installiert und keine eigenständige Netzwerkeinheit ist. Die Personal Firewall soll das Endgerät vor Zugriffen aus dem Netz (Internet, Unternehmensnetzwerk, Privathaushalt) schützen. Des Weiteren soll der Zugriff kontrolliert werden, damit Schadprogramme nicht von innen nach außen ins Internet kommunizieren bzw. Zugriffe von außen selektiv verhindert werden. Weitere Funktionen einer Personal Firewall sind der Paketfilter und Sandboxing. Beim Paketfilter werden alle Datenpakete kontrolliert, ob die Daten in den Headern den festgelegten Regeln entsprechen. Es soll hierbei nur die notwendigste Kommunikation zugelassen werden. Die Regeln sollen dementsprechend definiert werden. Das Sandboxing Verfahren läuft wie unter Antimalwareprogramme/Blacklisting beschrieben; so kann ohne größere Risiken ein Programm verwendet werden, das eventuell unsicher ist. (Vgl. FAQ, s.v. Personal Firewall)

Turn off Autorun

Um das System vor Viren und Malware zu schützen, ist es ratsam, die Autorun-Funktion des Systems abzuschalten. Dadurch wird verhindert, dass beim Einstecken einer externen Festplatte oder USB-Sticks beziehungsweise beim Einlegen einer CD die Malware automatisch auf das System eingespielt wird. Somit ist eine aktive Benutzerinteraktion notwendig.

Block p2p usage

Mittels einem Peer-to-Peer Netzwerk werden sehr viele Malwares verbreitet (Lt. Symantec sind etwa 90% aller verfügbaren Files mit Malware infiziert; 2008 wurden 10% der Malware via p2p Applikationen verbreitet [vgl. Kumar 2009].). Daher ist es für ein Unternehmen sehr ratsam, ebendiesen Datenverkehr zu blockieren.

P2p Würmer verbreiten sich beispielsweise, indem sie sich in die Freigaben von p2p-Clients kopieren; im File-Sharing Verzeichnis warten sie dann als Dateien aktueller Software oder von prominenten Personen getarnt auf den Download. (Vgl. Kasperky-Lexikon, s.v. P2P-Worm)

Educate users

Der Benutzer ist eine der größten Schwachstellen in Sachen IT-Sicherheit, weswegen in jedem/r Unternehmen bzw. Institution Wert darauf gelegt werden sollte, die Benutzer fortwährend im Umgang mit dem PC, vor allem aber mit den damit verbundenen Gefahren zu schulen. Die Benutzer sollen auf die Gefahren im Netz aufmerksam gemacht und sensibilisiert werden. Dadurch kann die Wahrscheinlichkeit, dass Links und Anhänge von unbekannten Mailabsendern gedankenlos geöffnet und auf jeden Link im Internet geklickt wird, verringert werden.

Über folgende Punkte bzw. Maßnahmen sollten die Benutzer informiert bzw. unterrichtet werden:

Passwörter

Jeder weiß es, doch nur selten einer hält sich daran: Die Verwendung starker Passwörter (Klein-/Großbuchstaben, Sonderzeichen, Nummern) sowie unterschiedlicher Passwörter für verschiedene Accounts erhöht die Sicherheit nicht nur des Benutzerkontos, sondern auch des Netzwerkes, und stellt sicher, dass nur ein Account kompromittiert wird und nicht mehrere. Hierfür können auch Passwortmanager-Programme wie KeePass verwendet werden.

Phishing Emails

Bei Phishing Emails ist besondere Aufmerksamkeit geboten, denn es werden immer bessere Phishing Emails entwickelt, die täuschend echt aussehen. Die Benutzer sollten darauf geschult werden, Webseiten auf dem von ihnen gewohnten Weg anzusurfen und nicht über Links in Emails, denn eine Firma wird nie nach sensiblen Daten in Emails fragen.

Bösartige Webseiten

Wie im Punkt Phishing Emails bereits erwähnt, sollte mit Links in Emails vorsichtig umgegangen werden, denn diese könnten die Anwender auf bösartige Webseiten

weiterleiten; auch beim eigenständigen Ansurfen von Webseiten sollten die Benutzer Vorsicht walten lassen. Durch ähnlich lautende Domänen von bekannten Webseiten, oder Pop-Ups werden Benutzer eventuell dazu gebracht, sensible Daten preiszugeben. Deshalb sollte der Benutzer Webseiten nicht gedankenlos ansurfen, sondern sowohl die Schreibweise in der URL als auch die gültige Zertifikatsanzeige im Browser beachten.

Herunterladen von Gratissoftware

Beim Herunterladen von vermeintlicher Gratissoftware ist die Wahrscheinlichkeit, mit dem Paket Schadsoftware herunterzuladen, die sich dann beim Ausführen oder Installieren im System einnistet, relativ hoch. Deshalb sollten die Anwender vor dem Herunterladen solcher Softwares mit der IT Abteilung in Kontakt treten und die Software überprüfen lassen. In vielen Firmen ist die Installation von Software durch den Benutzer jedoch nicht möglich.

Instant Messenger

Auch über Instant Messenger können Viren versendet oder Phishing-Versuche unternommen werden, weshalb auch die empfangenen Nachrichten kritisch beäugt werden sollten.

Schutz des Arbeitsplatzes

Ein weiterer – oft vernachlässigter Punkt – ist der Schutz des eigenen Arbeitsplatzes. Liegen eventuell vertrauliche Dokumente herum, die von nicht autorisierten Personen gelesen werden können? Wie ist der Computerdesktop geschützt – wird der PC gesperrt, wenn der Arbeitsplatz verlassen wird und wird darauf geachtet, dass bei der Passworteingabe keine unberechtigte Person zusieht?

Disconnect – call for support

Im äußersten Notfall hilft nur mehr den Computer vom Netzwerk zu trennen. Sollte sich der Anwender trotz allem eine Malware (z.B. Ransomware) einfangen und dies außerdem frühzeitig bemerken, so sollte er wissen, wie er den Computer schnellstmöglich vom Netzwerk trennen kann um einen größeren Schaden an am Netzwerk angeschlossene Computer zu verhindern und sofort die zuständige IT-Abteilung informieren.

Vom Netz

Sollte es nicht möglich sein, den Computer sinnvoll vor Malware zu schützen (EOL, …), so ist es ratsam, ihn nicht an das Netzwerk anzuschließen. Damit kann größtenteils verhindert werden, dass dieser Rechner infiziert wird. Außerdem kann so ausgeschlossen werden, dass er andere am Netzwerk angeschlossene Rechner infiziert. Diese Möglichkeit ist zwar

keine eigentliche Sicherheitslösung, sie trägt allerdings zur Sicherheit der im Netzwerk befindlichen Rechner bei.

Diese Lösung bringt starke Einschränkungen mit sich (unter anderem kann der Rechner dann nur mehr schwer überwacht werden, kein Datenaustausch mit Geräten über das Netzwerk), sollte in Ausnahmefällen jedoch dennoch in Erwägung gezogen werden.

Netzwerksegmentierung

Mit Hilfe der Netzwerksegmentierung werden Netzwerke physisch oder virtuell (mit Hilfe von VLANs) voneinander getrennt. Die Netzwerksegmentierung ermöglicht den Einsatz von Firewalls; dadurch kann der Zugriff der einzelnen Netzwerksegmente untereinander unterbunden werden. Sollte eine Malware einen Rechner in einem Netzwerksegment befallen, so können auch alle weiteren Rechner in diesem Segment infiziert werden bzw. hat die Malware Zugriff darauf. Rechner in anderen Netzwerksegmenten bleiben allerdings hiervon verschont. Dadurch wird für die Clients ein erhöhter Schutz geboten. Um den Schutz des einzelnen Rechners trotz Segmentierung gewährleisten zu können, muss trotzdem noch eine Endpoint-Security verwendet werden. Eine weiterführende Maßnahme in diesem Bereich wäre die Mikrosegmentierung (ein einzelnes Gerät wird durch eine Firewall abgeschottet).

2.5 Supported OS vs EOL

Nun können von den eben aufgezählten Schutzmaßnahmen nicht alle auch für EOL-Clients eingesetzt werden; andere sind immer nur der letzte Ausweg, wenn alles andere scheitern sollte. EOL-OS sind, wie in der Einleitung erwähnt, „End of Life"-Betriebssysteme, die an ihr Supportende gekommen sind (für Windows XP war dies der 08.04.2014) und daher vom Hersteller keine Updates mehr erhalten oder gewartet werden. Die folgende Tabelle soll einen Überblick darüber geben, welche Schutzmaßnahmen wann geeignet sind:

Tabelle 2-2: Schutzmaßnahmen supported OS vs EOL; Grün = Machbar und gefordert; Gelb = Gefordert, falls machbar; rot = wenn Gefordertes nicht machbar; \ = Nicht verfügbar

		supported OS	EOL
Schutzmaßnahmen	Antimalware		
	Whitelisting		
	Updates		
	Firewall		
	Personal Firewall		
	Turn-off Autorun		
	Block p2p usage		
	Educate Users		
	Vom Netz		

Grüne Kategorien sind machbar und gefordert, gelbe Kategorien sind gefordert, falls machbar (dies hängt davon ab, ob es Hersteller gibt, die Software für diese Schutzmaß-

nahme und dem vorhandenen Betriebssystem anbieten), rote Kategorien werden nur eingesetzt, falls das Geforderte nicht machbar ist, durchgestrichene Kategorien sind nicht verfügbar.

Anhand dieser Tabelle sieht man, dass der Schutz von EOL-Clients durchaus schwieriger wird und natürlich auch davon abhängt, wie alt das EOL-Betriebssystem bereits ist; denn je älter das Betriebssystem, umso unwahrscheinlicher wird es, dass es noch zufriedenstellende, gewartete Software dafür gibt.

3 Ansätze zur Verbesserung der Client-Security von Geräten mit EOL-Betriebssystemen

Im folgenden Kapitel werden Ansätze, wie Client-Security – speziell jene von Geräten mit EOL-Betriebssystemen – verbessert werden könnte, verfolgt. Um dies genauer darzustellen, wird zu Beginn ein allgemeines Konzept für die Kategorisierung und Analyse der vorhandenen IT-Infrastruktur in Bezug auf Sicherheitslösungen besprochen und dies anschließend am Beispiel der Tirol Kliniken erarbeitet.

Durch die sich stetig ändernden Anforderungen sowohl intern (zusätzliche Sicherheitsfunktionen gewünscht) als auch extern (neue Angriffsszenarien, zusätzlich bekannt gewordene Schwachstellen) unterliegt die IT-Sicherheit einem stetigen Wandel (vgl. Pohlmann & Blumberg 2004:192). Daher ändern sich auch die Schwerpunkte bei den verwendeten Sicherheitslösungen immer wieder.

3.1 Konzept für die Analyse der Client-Security in einem Unternehmen

Für die Realisierung von Sicherheitslösungen für EOL-Betriebssysteme benötigt es – speziell in großen Unternehmen mit vielen unterschiedlichen abzudeckenden Clients – Planung und Konzepte. Um jedoch ein Konzept zu erarbeiten, muss zunächst die vorhandene Client-Security im Unternehmen analysiert und kategorisiert werden. Nach der Ist-Analyse und Kategorisierung müssen die geeigneten Schutzmaßnahmen ausgesucht werden, um die kritischen Rechner zu schützen. Dies wird im Folgenden näher erläutert.

Zu Beginn ist es notwendig, sich Gedanken über die jeweilige Sicherheitssituation im Unternehmen zu machen. Die aktuelle Situation muss erhoben und analysiert werden. Dies kann auf verschiedenen Wegen erfolgen, wie Befragungen, Selbsterhebung oder durch Analyse vorhandener Dokumente. Auf jeden Fall ist es wichtig, die bestehende Infrastruktur so genau wie möglich zu kennen und anschließend zu kategorisieren, um so möglichst exakt eruieren zu können, welche Sicherheitslösungen wie für welche Problemfälle eingesetzt werden können.

Analyse der vorhandenen Infrastruktur

Je nach Spezifikationen und Ausrichtung der Unternehmen kann die vorhandene Infrastruktur selbstverständlich variieren, daher werden im Nachfolgenden allgemeinere Fragen formuliert, anhand derer eine IT-Infrastruktur in einem Unternehmen grundsätzlich analysiert werden könnte. Vermutlich wird jedoch immer eine Anpassung und/oder zusätzliche Fragestellungen je nach Unternehmen benötigt.

Tabelle 3-1: Mögliche Fragestellungen zur vorhandenen Infrastruktur

Fragestellung	Mögliche Antworten/Kategorien
Betriebssysteme und deren Nutzung	
Welche Betriebssysteme sind im Einsatz?	Windows, Linux, Mac
Welche BS-Versionen/Derivate sind im Einsatz?	Windows XP, 7, 10, Ubuntu, RedHat, Mac OS X, …
Werden Betriebssystem-Updates installiert?	Automatisch, sporadisch
Schutz	
Welche Produkte werden zum Schutz der Clients verwendet?	Malwareschutz, App Control, …
Welche weiteren Schutzmaßnahmen werden durchgeführt?	Regelmäßige Updates, User Education, …
Erfüllen alle Geräte die erforderten Schutzmaßnahmen?	Ja/Nein, Kategorisierung nach Erfüllung der Schutzmaßnahmen
Welche Rechner sind nicht ausreichend geschützt?	EOL, supported OS ohne Updates
Rechnerkonfigurationen	
Gibt es spezielle Rechner-Konfigurationen?	keine SW-Installation erlaubt
Sind alle Rechner gleich konfiguriert?	Admin-PC, User-PC
Müssen/Sind alle Rechner am Netzwerk angeschlossen (sein)?	Ja/nein

Anhand dieser Liste sollte es für ein Unternehmen möglich sein, die eigene IT-Infrastruktur je nach ihren Eigenheiten bzw. Gegebenheiten zu analysieren und einzuteilen sowie die aktuellen Probleme und optimierungsbedürftigen Maßnahmen auszumachen. Des Weiteren sollte sich herausstellen, ob weitere Produkte benötigt werden. Eventuell kristallisieren sich auch schon Lösungsansätze für die eruierten Probleme heraus.

Kategorisierung der Rechner

Um die vorhandenen und weiterhin benötigten Sicherheitslösungen für alle Rechner im Unternehmen möglichst übersichtlich zu gestalten, sollten die Rechner kategorisiert werden, wobei selbstverständlich die vorhandenen Schutzmaßnahmen berücksichtigt werden sollten. Dadurch sollte es möglich sein, jene Systeme zu definieren, die nicht oder unzureichend geschützt sind und daraufhin auch nach der Art des benötigten Schutzes einzuteilen.

Eine einfache Möglichkeit, Rechner zu kategorisieren, ist nach dem verwendeten Betriebssystem:

1. Mobile Devices OS
2. Windows
3. Linux
4. Mac
5. Embedded Systems

Die Hauptkategorien Windows, Linux und Mac könnten dann jeweils unterteilt werden in (1) innerhalb der Domäne und (2) außerhalb der Domäne. Bei der Unterkategorie *Innerhalb der Domäne* sollten alle Rechner die gleichen – standardisierten – Schutzmaßnahmen haben, weshalb diese Rechner das Label „OK“ erhalten. Die Unterkategorie *Außerhalb der Domäne* – die dann vermutlich Rechner inkludiert, die nicht oder unzureichend geschützt sind – kann dann nochmals unterteilt werden. Im vorliegenden Fall, wo es um Schutzmaßnahmen für EOL Betriebssysteme geht, wäre eine Unterteilung dahingehend interessant:

1. Clients mit supported OS
2. Clients mit EOL-OS
3. Etwaige Sonderfälle (wie Supported OS ohne Updates)

Eine weitere mögliche Unterteilung der Unterkategorie *Außerhalb der Domäne* wäre nach der Nutzung:

1. Allgemeine Bürorechner
2. Ohne besondere Zugriffsrechte
3. Administrationsrechner
4. Rechner mit speziellen Programmen
5. Home Office

Danach können die Rechner in diesen Unterkategorien je nach den vorhandenen Schutzmaßnahmen einem Label zugeteilt werden. Diese Labels müssen natürlich – abhängig von Art der Infrastruktur des Unternehmens– bestimmten Bedingungen folgen. Als Beispiel dient hierzu die Aufzählung unter Punkt 3.2.2.

Die anschließende Grafik soll die vorgeschlagene Kategorisierung (1. Möglichkeit) veranschaulichen.

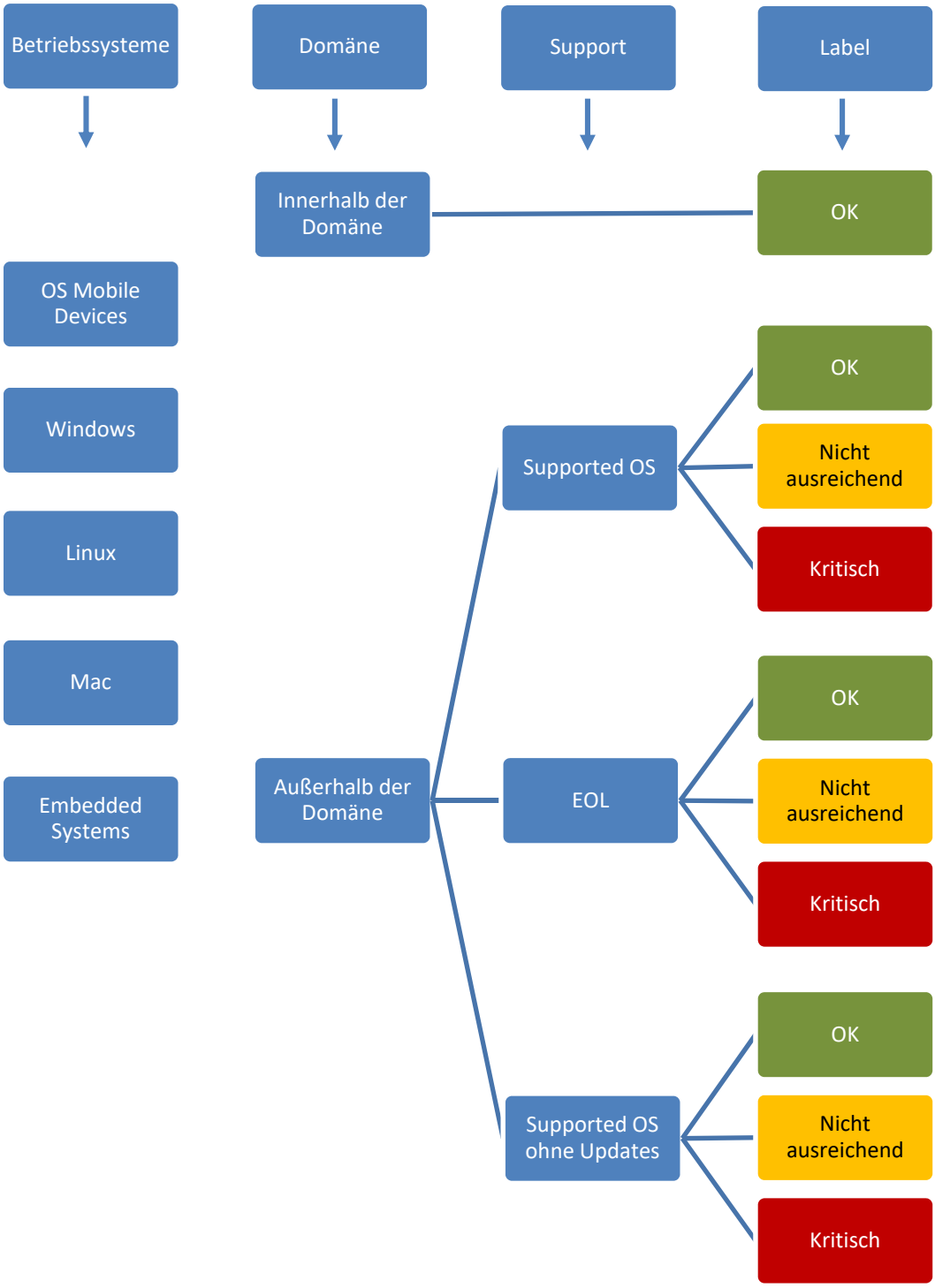

Abbildung 3-1: Mögliche Kategorisierung der Rechner

Nutzung vorhandener Schutzsoftware

Nach der Analyse der vorhandenen Infrastruktur und der Kategorisierung der Rechner sollte klar sein, welche Schutzprogramme bereits vorhanden sind und eventuell für die noch nicht oder unzureichend geschützten Rechner verwendet werden können, bzw. ob es noch weitere, noch nicht im Unternehmen genutzte Software benötigt (beispielsweise Whitelisting).

Einsatz neuer Schutzsoftware

Nachdem alle intern bereits vorhandenen Möglichkeiten ausgeschöpft sind, müssen neue Lösungsansätze abgewägt werden. Wichtige Punkte, die hierbei zu beachten sind, sind die folgenden:

- Kann die Software tatsächlich auf den gewünschten Rechnern (EOL?) installiert werden?
- Wie lange wird die Software vom Hersteller gewartet? Gibt es bereits ein angekündigtes Supportende?
- Wie hoch sind die Kosten, die dafür aufgewendet werden müssen (Lizenzkosten, zusätzliche Hardwarekosten)?
- Wie hoch ist der Personalaufwand für die Tests und die eigentliche Installation? Gibt es genug Kapazität, um die Umstellung zufriedenstellend durchzuführen?

Die letzten zwei Punkte hängen natürlich auch in starkem Maße von der Größe der IT-Infrastruktur und des Unternehmens ab.

3.2 IST-Analyse in den Tirol Kliniken

In diesem Kapitel werden zunächst die vorhandenen allgemeinen Schutzmaßnahmen der Tirol Kliniken und die Besonderheiten in der IT vorgestellt, um danach die Rechner der Tirol Kliniken anhand der oben ausgearbeiteten Kategorien zu analysieren und einzuteilen.

3.2.1 Vorhandene allgemeine Schutzmaßnahmen in den Tirol Kliniken

Durch die Kooperation mit der Medizinischen Universität Innsbruck sind auch die Tirol Kliniken Mitglied des österreichischen Datennetzes für Wissenschaft: dem ACOnet[1]. Das

[1] Das Austrian Academic Computer Network, ein Hochleistungsdatennetz für gemeinnützige Einrichtungen der Wissenschaft, Forschung, Bildung und Kultur, wird vom zentralen Informatikdienst der Universität Wien in Kooperation mit ACOnet-Teilnehmern betrieben. (Vgl. ACOnet)

ACOnet wiederum bietet den Tirol Kliniken weiteren Zugang zum pan-europäischen Wissenschaftsnetz GÉANT[2] und zum Internet.

Die Tirol Kliniken setzen folgende Schutzmaßnahmen in den verschiedenen Bereichen Server, Internet und Clients ein:

Tabelle 3-2: Schutzmaßnahmen in den Tirol Kliniken im Überblick;

System	Schutzsystem	Hersteller
Internet	Corporate Firewall	Barracuda-Netfence
	Malwareschutz Mail	McAfee E-Mail-Security-Appliance
	Malwareschutz HTTP	McAfee Web-Security-Appliance
	VPN: IP-Sec-Zugang	Barracuda
Windows Server	Malwareschutz	Microsoft Forefront
	Updateservice	Microsoft Windows Server Update Services
	Firewall	Microsoft
Unix Server	Keine	Keine
Linux Server	Keine	Keine
Windows Clients	Malwareschutz	McAfee VirusScan Enterprise
	Updateservice	Microsoft Windows Server Update Services, SCCM
	Windows 10 Firewall*	Microsoft
Mac OS Clients	Keine	Keine
Linux Clients	Keine	Keine
Allgemein	Educate Users	

*nur lokal aktiv

Die Betriebssysteme Linux und Mac OS werden in den Tirol Kliniken kaum bei Clients eingesetzt, da der Fokus auf der Windows-Domäne liegt. Daher werden im Folgenden nur die eingesetzten Schutzmaßnahmen anhand der Windows-BS-Derivate dargestellt:

[2] GÈANT bietet mehr als 50 Millionen Benutzern – darunter jene des ACOnet – einen leistungsfähigen und resilienten pan-europäischen Backbone und vernetzt so Europas nationale Forschungs- und Wissenschaftseinrichtungen. (Vgl. GÈANT)

Tabelle 3-3: Vorhandene Schutzmaßnahmen für Rechner der Windows-Domäne

Betriebssystem	Schutzmaßnahme							
		Internet			Clients			
		Malwareschutz Mail	Corporate Firewall	Malwareschutz HTTP	Malwareschutz	Firewall	Updateservice	Kein Netzwerkzugang	Internetzugang blockieren
	Windows 7	x	x	x	x		x	x#	x#
	Windows 10	x	x	x	x	x*	x	x#	x#
	Windows XP	x	x	x				x#	x#

* nur teilweise aktiv (Block Cortana)

\# teilweise implementiert

EOL-Endgeräte sind, wie auch in vielen anderen IT-Umgebungen, in den Tirol Kliniken nicht erwünscht, wie man aber erkennen kann, sind auch solche Geräte (immer) noch im Einsatz. Dies geschieht aus den verschiedensten Gründen; oft ist es jedoch aufgrund der Spezifikationen und Einschränkungen der MT-Geräte, mit denen die PCs verbunden sind, in Bezug auf Updates etc. In den Tirol Kliniken werden jedoch laufend Verbesserungen angestrebt, um die Sicherheit der IT-Infrastruktur hinsichtlich der möglichen Gefahrenquellen (wie in Kapitel 2.3 näher definiert) zu gewährleisten.

3.2.1.1 Standardgeräte versus Nicht-Standardgeräte

Für alle Standardgeräte sind die Schutzmaßnahmen am neuesten Stand. Diese sind alle (1) mit einer aktuellen OS-Version versehen, (2) mit aktuellen Malware-Schutzprogrammen ausgestatten, (3) im generellen Update-Zyklus der Tirol Kliniken, (4) in der Active Directory der Tirol Kliniken, und (5) von der unternehmensinternen IT-Abteilung betreut.

Allerdings gibt es im Netzwerk der Tirol Kliniken zahlreiche Geräte (Medizintechnik, Haustechnik), die nicht oder nur teilweise mit den oben genannten Maßnahmen geschützt werden können, die im Folgenden als „Nicht-Standardgeräte“ bezeichnet werden.

3.2.1.2 Medizin- und haustechnische Geräte („Nicht-Standardgeräte“)

Obwohl das Ziel ist, dass sämtliche in den Tirol Kliniken im Einsatz befindlichen IT-Systeme bzw. Geräte mit den gleichen Standards geschützt werden, ist dies sehr schwierig. Häufig ist es nicht möglich, die gelieferten medizintechnischen Systeme den Sicherheitsmaßnahmen anzupassen (Updatezyklus, Schutz gegen Schadsoftware etc.), da ansonsten

die Zertifizierungen oder die Garantie ungültig werden könnten und die Hersteller dies selbstverständlich vermeiden möchten. Des Weiteren befürchten die Hersteller, dass die Geräte nach einer Anpassung durch einen Kunden nicht mehr einwandfrei funktionieren. Solche Rechner werden im Folgenden als Supported OS ohne Updates bezeichnet: sie sind mit einem noch unterstützten Betriebssystem, auf denen aber keine Updates des Betriebssystems oder oft auch weitere Software installiert werden dürfen, versehen. In dieser Kategorie befindliche Rechner waren bislang gleich handzuhaben wie Rechner in der Kategorie Supported OS. Falls möglich, gehört hier auf alle Fälle ein Malwareschutz (Blacklisting/Whitelisting) installiert und um bestehende und zukünftige Sicherheitslücken zu schließen, auch der automatische Updatemechanismus des Betriebssystems eingeschaltet. Sollte der Hersteller des Gerätes dies nicht tolerieren, so war bisher das Gerät vom Netz zu nehmen, um die bestehenden Rechner im Netzwerk nicht zu gefährden.

Insellösungen werden oft bei Rechnern eingesetzt, die meist von den Herstellern selbst mit dem Gerät mitgeliefert oder bereits als embedded system im Gerät integriert sind. Hier können keine USB-Anschlüsse, CD-ROM Laufwerk, Firewire-Anschlüsse oder dergleichen verwendet werden, um Daten auf das Gerät bzw. von dem Gerät zu kopieren, oder die Anschlüsse sind für den Anwender nicht ausgeführt und sind nur für Servicetechniker zugänglich. Des Weiteren sind diese Computer nur mit dem Gerät verbunden und sind auch nicht am Netzwerk angeschlossen. Die Rechner in dieser Kategorie bedürfen keines Schutzes, da diese wie oben beschrieben nicht im Netzwerk integriert sind und weder eine Malware von noch auf die Rechner kopiert werden kann. Somit können Insellösungen bedenkenlos vernachlässigt werden.

Die MT-Systeme in den Tirol Kliniken bestehen allerdings oft aus einem Geräteverbund mit unterschiedlichen OS und müssen zusätzlich mit anderen Systemen (z.B. KIS) kommunizieren. Virenschutz und Updates auf aktuelle OS-Versionen wären daher unerlässlich für einen ausreichenden Schutz vor Angriffen oder Schadsoftware.

Haustechnikgeräte wiederum (Sensoren, Zutrittskontrolle, Zeiterfassung, …) sind natürlich ebenfalls zahlreich in einer klinischen Umgebung vertreten und sind oft nur mit einer Firmware ausgestattet (und dabei ist es oft unklar, ob diese Firmwares noch supported oder bereits EOL sind). Hier ist es oft unmöglich bestimmte Schutzmaßnahmen (wie Antivirus-Programm oder Application Control) zu installieren.

3.2.2 Analyse und Kategorisierung in den Tirol Kliniken

Im Folgenden werden nur Windows-Rechner näher betrachtet, da in den Tirol Kliniken die restlichen Betriebssysteme separat verwaltet werden und der Autor dieser Arbeit vorwiegend mit der Verwaltung dieser Rechner betraut ist.

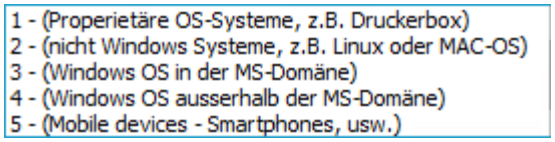

Abbildung 3-2: Security classes der Tirol Kliniken (Quelle: Switch Manager, Tirol Kliniken)

Es soll trotzdem zu Beginn die bereits vorhandene Grundeinteilung der Tirol Kliniken (siehe Abbildung 3-2) inklusive der Anzahl der Clients übersichtsweise in einer Tabelle dargestellt werden. Anhand dieser Tabelle können die Fragen unter dem Punkt Betriebssysteme und deren Nutzung der Tabelle 3-1 nun teilweise beantwortet werden. Die Tabelle berücksichtigt dabei auch – soweit möglich – die verschiedenen Betriebssystem-Versionen, die mit Stand 11.05.2017 in den Tirol Kliniken im Umlauf sind. Da der Fokus der Tirol Kliniken auf der Windows-Domäne liegt, war es leider nicht möglich, genaue Zahlen für die verschiedenen Versionen der Nicht-Windows-Systeme zu eruieren.

Tabelle 3-4: Clients anhand der Security classes der Tirol Kliniken

Security Class	Betriebssystem / Systeme	Versionen	Anzahl Clients
Proprietäre OS-Systeme	Druckerboxen, MT-/HT-Systeme, Kameras, VoIP-Telefone	CatOS, iOS, GNU, OSEK	6481
Nicht Windows-Systeme	Mac	Mac OS-Familie	310
	Linux	Debian, Red Hat, SuSe	
	Unix	AIX, HP-UX, Solaris	
Windows OS innerhalb der Domäne	Supported OS	Win 10	335
		Win 7	8290
	EOL	Win XP	6
Windows OS außerhalb der Domäne	Supported OS (mit und ohne Updates)	Win 7	804
		Win 10	
	EOL	Win 2000	
		Win Vista	
		Win XP	
Mobile Devices		Apple iOS, Android, Symbian, Win7	113

Wie aus der obigen Tabelle ersichtlich wird, können die Rechner außerhalb der Domäne (der Abteilungen MT, HT und ITK) nicht exakt auf ihre Betriebssysteme aufgeteilt werden. Was genauer bekannt ist, sind die Clients, die durch die MT-Abteilung betreut werden.

Tabelle 3-5: Anzahl Windows-Rechner MT/HT/ITK-Abteilung außerhalb der Domäne

Abteilung	Betriebssystem	Anzahl
HT-Abteilung		**26**
ITK-Abteilung		**108**
MT-Abteilung	**Gesamt**	**670**
	Supported OS (mit und ohne Updates)	255
	Win XP	295 (238 embedded systems)
	Win Vista	3
	Win 2000	5
	Win CE	4
	Win NT	3
	Nicht definiert	105

Anhand dieser Grundeinteilung kann nun die weitere Analyse und Kategorisierung der Rechner (Windows OS Innerhalb und Außerhalb der Domäne) vorgenommen werden. Dabei dienen Abbildung 3-1, die unter Punkt 3.1 erstellt wurde, und die unter Tabelle 3-3 angeführten Schutzmaßnahmen für die Clients der Tirol Kliniken als Anhaltspunkt, um die Rechner anhand der vorhandenen Schutzmaßnahmen zu kategorisieren. Die folgenden vier Schutzmaßnahmen werden für die Kategorisierung berücksichtigt:

- Antivirus-Programm
- Windows Updates
- Internetzugang blockiert
- Netzwerkzugang blockiert

Zu Beginn werden die Bedingungen für die verschiedenen Labels in Bezug auf die oben erwähnten Schutzmaßnahmen der Tirol Kliniken definiert.

Label OK:

Um das Label *OK* zu erhalten, müssen Rechner sowohl Antiviren-Software als auch die Windows-Updates aktiviert haben. Fehlt eine dieser zwei Schutzmaßnahmen, so sollte diese nach Möglichkeit sofort nachinstalliert werden. Als Alternative können auch Rechner ohne Netzwerkzugang dem Label *OK* zugeordnet werden. Dieser Fall wird in den Erläuterungen zu Tabelle 3-6 näher besprochen.

Label Nicht Ausreichend:

Für das Label *Nicht Ausreichend* muss mindestens eine der folgenden Schutzmaßnahmen aktiv sein: Windows Updates, Antiviren-Programm, Internetzugang blockiert. Während das Blockieren des Internetzugangs wohl das Label *Nicht Ausreichend* ermöglicht, so ist diese Schutzmaßnahme nicht genug, um das Label *OK* rechtzufertigen, da sie zwar Schutz bietet, jedoch nicht genug Sicherheit gewährleistet. Ein Rechner mit diesem Label erhält

zwar nicht die höchste Priorität, sollte jedoch trotzdem besser geschützt werden, um so viele Eventualitäten wie möglich abzudecken.

Label Kritisch:

Fehlen Antivirus-Programm, Windows Updates und der blockierte Internetzugang, so ist der Rechner als *Kritisch* einzustufen, und so schnell als möglich besser abzusichern.

Die folgende Tabelle soll die verschiedenen Kombinationsmöglichkeiten der Schutzmaßnahmen für die jeweiligen Kategorien (EOL-OS, Supported OS ohne Updates, Supported OS) aufzeigen und die Entscheidung, welches Label der Rechner erhält, erleichtern. Die Entscheidungsmöglichkeiten für die Kategorie Supported OS sind nur der Übersicht halber aufgelistet. Es ist natürlich auch hier möglich, dass es Rechner gibt, die die Label *Kritisch* oder *Nicht Ausreichend* erhalten, jedoch sollte es in diesen Fällen einfach möglich sein, das Antivirus-Programm bzw. Windows Updates zu aktivieren, wodurch diese Rechner dann das Label OK erhalten.

Tabelle 3-6: Labelling der Rechner - Entscheidungsmöglichkeiten

Supported OS ohne Updates				
Windows Updates	Antivirus	Internetzugang blockiert	Netzwerkzugang blockiert	**Label**
✗	✗	✗	✗	Kritisch
✗	✓	✗	✗	Nicht ausreichend
✗	✗	✓	✗	Nicht ausreichend
✗	✓	✓	✗	Nicht ausreichend
✗	✗	✗	✓	OK
EOL				
Windows Updates	Antivirus	Internetzugang blockiert	Netzwerkzugang blockiert	**Label**
✗	✗	✗	✗	Kritisch
✗	✗	✓	✗	Nicht ausreichend
✗	✗	✗	✓	OK
Supported OS				
Windows Updates	Antivirus	Internetzugang blockiert	Netzwerkzugang blockiert	**Label**
✗	✗	✗	✗	Kritisch
✓	✗	✗	✗	Nicht ausreichend
✗	✓	✗	✗	Nicht ausreichend
✓	✓	✗	✗	OK
✗	✗	✓	✗	Nicht ausreichend
✓	✗	✓	✗	Nicht ausreichend
✗	✓	✓	✗	Nicht ausreichend
✓	✓	✓	✗	OK
✗	✗	✗	✓	OK

Erläuterungen zu Tabelle 3-6:

Alle Kombinationen, die den blockierten Netzwerkzugang inkludieren, wurden zu einer Zeile zusammengefasst, da in diesem Fall alle weiteren zusätzlichen Optionen nicht notwendig sind (kein Netzwerkzugang bedeutet, dass keine Updates heruntergeladen werden können, die Antivirus-Software nicht täglich aktualisiert werden kann und der Internetzugang ebenfalls nicht möglich ist). *Netzwerkzugang blockiert* erhält grundsätzlich das Label *OK*, jedoch sollte man hier beachten, dass bei diesen Rechnern dann auch die Benutzung von Wechselmedien unterbunden werden sollte, damit auch dieser Weg für etwaige Malware geschlossen ist (siehe Insellösung).

Den Netzwerkzugang zu blockieren ist jedoch grundsätzlich nicht erwünscht als Option, und zwar aus den folgenden Gründen:

- Es gibt zahlreiche Einschränkungen für die User (kein Serverzugriff, kein Internetzugriff etc.) und auch für Programme, da es oft notwendig ist, dass diese Zugang zum Netzwerk bzw. Server haben. So benötigt zum Beispiel das PACS Zugriff zum Server, um die Dateien zu sichern.
- Alle Rechner, die nicht am Netzwerk hängen, sind aus technischen Gründen für die Techniker der IT-Abteilung der Tirol Kliniken nicht sichtbar. Dadurch sind diese Rechner für die Techniker nicht managebar: jeder individuelle Rechner kann nur bzw. muss „manuell“ vor Ort gewartet werden.

Je größer die Anzahl der Clients, umso aufwendiger wird natürlich die Analyse der einzelnen Rechner. Eine genaue und korrekte Inventarisierung, geführt durch die IT-Abteilung, wird dabei helfen, eine effiziente Lokalisierung der tatsächlich betroffenen individuellen Rechner vorzunehmen. Im Falle der Tirol Kliniken wird die Kategorisierung dadurch erschwert, dass die meisten Clients mit EOL-Betriebssystem nicht in ihrem System aufscheinen und dadurch händisch ausgewertet werden müssen.

Die folgende Tabelle soll einen Einblick darin schaffen, wie eine Kategorisierung der einzelnen Rechner aussehen würde:

Host	Gerätekategor	OS	Windows Updates	Antivirus	Internetz. blockiert	Netzwerkz. blockiert	Label
MT00000024	Ultraschall	XP	✗	✗	✓	✗	Nicht ausreichend
MT00000020	Steuerrechner 3D Scanner	XP	✗	✓	✗	✗	Nicht ausreichend
MT00000097	Mammographie	XP	✗	✗	✗	✗	Kritisch
MT00000131	Notebook Gefäßstation	XP	✗	✓	✓	✗	Nicht ausreichend
MT00000534	Massenspektrometer	XP	✗	✗	✗	✗	Kritisch
MT00000849	Durchflusszytometer	Win Vista	✗	✓	✓	✗	Nicht ausreichend
MT00000634	Mikroskop	Win CE	✗	✗	✗	✗	Kritisch
MT00000519	Sterilisator	NT	✗	✗	✓	✗	Nicht ausreichend
MT00000681	Durchflusszytometer	Win 2000	✗	✗	✗	✗	Kritisch
MT00000698	Ultraschall	Win 2000	✗	✗	✓	✗	Nicht ausreichend
MT00000013	Ergo-Spirometrie	Win 7	✗	✓	✓	✗	Nicht ausreichend
MT00000327	PCR-System	Win 7	✗	✗	✗	✗	Nicht ausreichend

Abbildung 3-3: Beispieltabelle anhand der Rechner der Tirol Kliniken mit den aktuellen Schutzmaßnahmen

In Abbildung 3-4 wird die eben ausgearbeitete Kategorisierung noch einmal anschaulich und übersichtlich dargestellt.

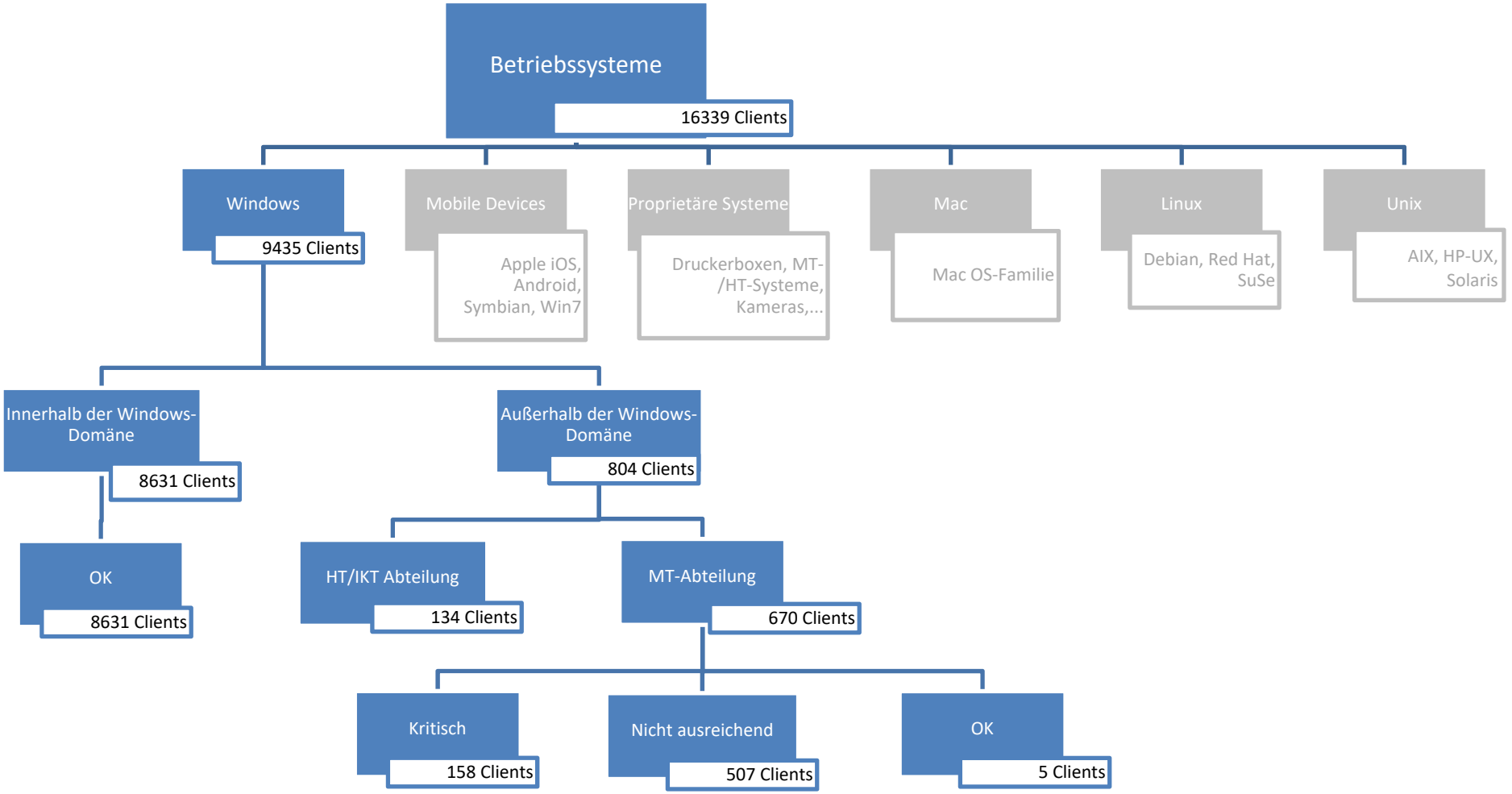

Abbildung 3-4: Kategorisierung der Rechner

Somit kann nach Abschluss unserer Analyse der zu Beginn ausformulierte Fragebogen zufriedenstellend beantwortet werden:

Tabelle 3-7: Beantworteter Fragebogen

Fragestellung	Mögliche Antworten/Kategorien
Betriebssysteme und deren Nutzung	
Welche Betriebssysteme sind im Einsatz?	Windows (Linux, Mac)
Welche BS-Versionen/Derivate sind im Einsatz?	Windows XP, Vista, 2000, CE, NT, 7, 10
Werden Betriebssystem-Updates installiert?	Automatisch bei allen Rechnern, bei denen es aktiviert ist
Schutz	
Welche Produkte werden zum Schutz der Clients verwendet?	McAfee VirusScan Enterprise V8.8
Welche weiteren Schutzmaßnahmen werden durchgeführt?	Regelmäßige Updates, Internet blockiert, Netzwerkzugang blockiert
Erfüllen alle Geräte die erforderten Schutzmaßnahmen?	Nein, siehe Tabelle 3-6
Welche Rechner sind nicht ausreichend geschützt?	EOL, Sonderfälle wie supported OS ohne Updates
Rechnerkonfigurationen	
Gibt es spezielle Rechner-Konfigurationen?	supported OS ohne Updates
Sind alle Rechner gleich konfiguriert?	Nein; Admin-PC, User-PC, MT, HT
Müssen/Sind alle Rechner am Netzwerk angeschlossen (sein)?	Es sind nicht alle angeschlossen; es wird jedoch angestrebt, dies zu tun.

Es stellt sich heraus, das EOL-OS Rechner (vornehmlich Windows XP) und Supported OS ohne Updates unzureichend geschützt sind. Ebenso sind Rechner außerhalb der Domäne nicht einfach erfassbar.

Zusätzlich zur Implementation der vorhandenen Schutzmaßnahmen sind mögliche Lösungsansätze für eine bessere Sicherung der unzureichend geschützten Rechner *Application Control* und *Netzwerksegmentierung*. Weiters könnte eine Monitoring-Software wie *NexThink End-User IT Analytics* einen übergeordneten Blick aufs Ganze ermöglichen.

Es kann auch beantwortet werden, wie viele Rechner nun eine Aktion erfordern (siehe Übersicht Abbildung 3-4). Im Laufe dieser Arbeit wurden lediglich Tests an einigen wenigen Rechnern durchgeführt, es wurde jedoch noch nicht flächendeckend der Schutz der EOL-OS Clients in Angriff genommen.

3.3 Möglichkeiten der Verbesserung der Client-Security in den Tirol Kliniken

Nachdem die Rechner nun kategorisiert und anhand der eingesetzten Schutzmaßnahmen den zuvor definierten Labels zugeteilt wurden, kann überlegt werden, welche weiteren Schutzmaßnahmen sinnvoll wären, um den Schutz der Clients mit den Labels *Kritisch* und *Nicht ausreichend* zu gewährleisten.

In den Tirol Kliniken wurden folgende Maßnahmen ausgewählt, um einen besseren Schutz zu gewährleisten:

- McAfee Application Control (Whitelisting)
- Netzwerksegmentierung in Verbindung mit Firewall
- NexThink End-User IT Analytics

In Kapitel 4 wird näher auf den Einsatz von *McAfee Application Control*, und warum dieses Produkt in den Tirol Kliniken gewählt wurde, eingegangen. Dieses Programm wurde unter anderem auch dafür entwickelt, um Rechner, die nicht aktualisiert werden können bzw. sollten (aus welchen Gründen auch immer), zu schützen. Deswegen bietet sich speziell ein Application Control Programm dazu an, EOL-Clients oder auch Supported OS-Clients ohne Updates zu schützen, da diese weder Windows Updates erhalten können, um Bugs zu beseitigen und Sicherheitslücken zu schließen, noch oft auch kein Antiviren-Programm mehr zur Verfügung steht, dass regelmäßig gewartet wird. Der Support für die Version 8.8 des VirusScan Enterprise von McAfee, die in den Tirol Kliniken verwendet wird, wurde für Windows XP mit 31.12.2015 eingestellt. Obwohl McAfee seit März 2017 einen Extended Support (erweitert bis 31.12.2017) für dieses Produkt anbietet, hat man sich dazu entschieden Alternativen einzusetzen. Für die Tirol Kliniken ist besonders für medizintechnische Geräte – die oft als supported OS ohne Updates geführt werden – eine weitere Schutzmaßnahme wichtig. Laut einer Stellungnahme des TÜV Austria vom 25. August 2015 kann das Programm McAfee Application Control hier sehr wohl zum Einsatz kommen, da es laut Unterlagen ein offizielles, zugelassenes Programm ist, und dezidiert auch Medizinprodukte angesprochen werden (vgl. TÜV 2015).

In den Tirol Kliniken hat man sich dazu entschieden, die *Netzwerksegmentierung* nicht flächendeckend auf allen Clients auszurollen, da dies einen erhöhten administrativen Aufwand darstellt. Stattdessen geht man nun dazu über, haus- und medizintechnische Geräte, auf denen keine Endpoint Security installiert werden kann, in Netzwerksegmenten miteinander zu verbinden. Die einzelnen Segmente werden durch Firewalls getrennt. Das heißt nun im Konkreten, dass zum Beispiel Temperaturfühler nur mit den dazugehörigen Servern kommunizieren können. Die Server wiederum werden aber durch einen Malwareschutz und regelmäßigen Windows Updates geschützt. Dadurch kann die eventuelle Ausbreitung von Malware zumindest eingeschränkt werden.

Bei *NexThink End-User IT Analytics* wird der Client (NexThink Collector) auf den Rechnern der User installiert. Der Collector Agent ist ein Kernel Treiber und sammelt verschiedenste Daten der Rechner wie Netzwerkverbindungen, Programmausführungen und schickt diese zur Analyse an den Server (NexThink Engine) weiter. Mit Hilfe dieser Daten listet NexThink unter anderem alle IT-Services auf, wie diese benutzt werden und wie gut die IT Infrastruktur funktioniert. Weiters kann ein ungewöhnliches Verhalten am Client analysiert werden. Der NexThink Collector dient jedoch hauptsächlich zur Datenakquisition und -analyse und ist daher nicht direkt eine Schutzmaßnahme in Bezug auf Endpoint security. (Vgl. NexThink)

Im Nachfolgenden werden daher nur die Netzwerksegmentierung und McAfee Application Control berücksichigt.

Die folgenden Tabellen sollen nun aufzeigen, welche Kombinationsmöglichkeiten es zum Erreichen des Labels *OK* der verschiedenen kritischen Labels gibt. Dabei wird das Augenmerk in dieser Arbeit hauptsächlich auf die EOL-OS Clients und die Clients mit Supported OS ohne Updates gelegt. Es werden nur die kritischen Fälle und deren Lösungskombinationen dargestellt, da alle Fälle des Labels *Nicht Ausreichend* im Prinzip auch in diesen Tabellen enthalten sind.

Tabelle 3-8: Problem Supported OS ohne Updates

Supported OS ohne Updates				
Windows Updates	Antivirus	Internetzugang blockiert	Netzwerkzugang blockiert	**Label**
✕	✕	✕	✕	Kritisch

Tabelle 3-9: Problem: EOL-OS

EOL				
Windows Updates	Antivirus	Internetzugang blockiert	Netzwerkzugang blockiert	**Label**
✕	✕	✕	✕	Kritisch

Es gibt nun mehrere Möglichkeiten, in diesen zwei Fällen das Label *OK* zu erreichen. Einerseits kann geprüft werden, ob es möglich ist, vorhandene Schutzmaßnahmen einzusetzen; andererseits können die oben erwähnten neuen Schutzmaßnahmen – McAfee Application Control und Netzwerksegmentierung – hinzugezogen werden.

Tabelle 3-10: Supported OS ohne Updates - Lösungsmöglichkeiten

Supported OS ohne Updates							
	Windows Updates	Antivirus	Internetzugang blockiert	Netzwerkzugang blockiert	Netzwerksegmentierung	App Control	**Label**
Lösung 1	✗	✓	•	✗	✓	✗	OK
Lösung 2	✗	•	•	✗	•	✓	OK
HT/MT	✗	✗	•	✗	✓	✗	OK
Sonderfall	✓	✓	•	✗	•	•	OK

Tabelle 3-11: EOL-OS - Lösungsmöglichkeiten

EOL							
	Windows Updates	Antivirus	Internetzugang blockiert	Netzwerkzugang blockiert	Netzwerksegmentierung	App Control	**Label**
Lösung	✗	✗	•	✗	•	✓	OK
HT/MT	✗	✗	•	✗	✓	✗	OK

Erläuterungen zu Tabelle 3-10 und Tabelle 3-11

Lösungen: Um das Label *OK* zu erhalten, benötigen die aufgeführten kritischen Fälle entweder McAfee Application Control ODER die Netzwerksegmentierung in Kombination mit einer anderen ausreichenden Schutzmaßnahme (Antivirus). Alle Schutzmaßnahmen, die mit dem Kreis gekennzeichnet sind, sind optional und können als weitere Schutzmaßnahme hinzugefügt werden, sind aber für das Label *OK* nicht notwendig. Das Blockieren des Internetzugangs sollte auch bei Geräten, die diesen nicht benötigen, immer in Betracht gezogen werden, da so ein erhöhter Schutz des Clients erreicht wird.

HT/MT: Bei bestimmten Geräten, z.B. in der Haustechnik (Sensoren, Zutrittskontrolle, Zeiterfassung, …) oder Medizintechnik (z.B. Ultraschallgeräte, Mikroskope, DICOM-Box oder ähnliches) ist es oft nur möglich den Internetzugang zu blockieren und eine Netzwerksegmentierung einzusetzen, daher wird für diese Geräte diese Kombination als Label *OK* erlaubt, bei Clients hingegen ist diese Kombination *Nicht Ausreichend*, da es noch keinen genügenden Schutz für die Clients bietet.

Sonderfall: Bei den Supported OS ohne Updates gibt es noch einen Sonderfall: falls es nach Rücksprache mit dem Hersteller erlaubt wird, Windows Updates zu aktivieren, so ist dies immer zu machen; in Kombination mit Antivirus sind dann auch diese Clients als *OK* einzustufen (siehe Kategorie supported OS).

Wie ersichtlich ist, gibt es je nach Art der Rechner unterschiedliche Möglichkeiten, das Label *OK* zu erreichen. Sobald aber Application Control eingesetzt wird, sind zwar weitere Schutzmaßnahmen von Vorteil, jedoch nicht unbedingt notwendig.

Im Anschluss wird noch einmal die bereits gezeigte Beispielliste (Abbildung 3-3) betrachtet, wie die Rechner der Tirol Kliniken das Label *OK* erhalten können:

Host	Geräte-kategorie	OS	Windows Updates	Anti-virus	Internetz. blockiert	Netzwerkz. blockiert	Netzwerk-segmentierung	App Control	Label
MT00000024	Ultraschall	XP	✗	✗	✓	✗	✓	✗	OK
MT00000020	Steuerrechner 3D Scanner	XP	✗	✓	✗	✗	✗	✓	OK
MT00000097	Mammographie	XP	✗	✗	✓	✗	✓	✗	OK
MT00000131	Notebook Gefäßstation	XP	✗	✓	✓	✗	✗	✓	OK
MT00000534	Massenspektrometer	XP	✗	✗	✗	✗	✗	✓	OK
MT00000849	Durchflusszytometer	Win Vista	✗	✓	✓	✗	✗	✓	OK
MT00000634	Mikroskop	Win CE	✗	✗	✓	✗	✓	✗	OK
MT00000519	Sterilisator	NT	✗	✗	✓	✗	✓	✗	OK
MT00000681	Durchflusszytometer	Win 2000	✗	✗	✓	✗	✗	✓	OK
MT00000698	Ultraschall	Win 2000	✗	✗	✓	✗	✗	✓	OK
MT00000013	Ergo-Spirometrie	Win 7	✗	✓	✓	✗	✗	✓	OK
MT00000327	PCR-System	Win 7	✓	✓	✗	✗	✗	✗	OK

Abbildung 3-5: Beispieltabelle mit den geforderten Schutzmaßnahmen für das Label OK

Aus der Beispieltabelle wird ersichtlich, dass es unterschiedliche Möglichkeiten gibt, um die Rechner ausreichend zu schützen, auch abhängig von den Maßnahmen, die bei dem jeweiligen Client überhaupt möglich sind. So sind zum Beispiel die Systeme für Ultraschall, Mammographie, Mikroskop und Sterilisator Systeme, an denen kein Programm installiert werden kann (siehe Sonderfall HT/MT bei Tabelle 3-10 und Tabelle 3-11), weswegen das Blockieren des Internets und die Netzwerksegmentierung hier ausreichen muss.

Überblick über den angenommenen finanziellen und personellen Aufwand

Für die Implementation der geplanten Schutzmaßnahmen benötigt es natürlich Zeit und Geld. Da auch diese wichtig sind für eine gute Planung, wird im Nachfolgenden kurz darauf eingegangen.

Personal

Die Anzahl der eigentlichen XP-Rechner (57) hält sich in Grenzen, es sind aber weitaus mehr Rechner bzw. Systeme, die überprüft und aktualisiert werden müssen. Es wird damit gerechnet, dass nur ein Mitarbeiter die XP-Rechner sukzessive in Bezug auf deren Schutzmaßnahmen aktualisiert, sofern jedenfalls möglich. Es wird mit drei Rechnern pro Tag und Mitarbeiter gerechnet (etwa 3-4h pro Rechner). Frühere Projekte hatten gezeigt, dass es meist notwendig ist, ein Teil der Arbeitszeit für Problemfeststellung und -lösung aufzuwenden, daher geht man im vorliegenden Fall davon aus, dass an vier Tagen die Woche Rechner umgestellt werden und ein Werktag

für die Behebung diverser Probleme vorhanden ist. Anhand dieser Daten können nun die ungefähr benötigten Manntage berechnet werden:

Tabelle 3-12: Berechnung benötigte Manntage

Rechner gesamt	665
Stunden/Rechner	3
Rechner/Tag	3
Projektstunden gesamt	1995
Urlaubsstunden des Mitarbeiters (200h pro Jahr)	191,83
Krankenstandsstunden des Mitarbeiters (Statistik Austria – 2015: 12,7d)	12,18
Zu kalkulierende Gesamtstunden des Mitarbeiters	2199,01
Benötigte Manntage	**274,88**

Kosten

Aktuell beträgt der Listenpreis für eine unbefristete Lizenz für McAfee Application Control für PCs 75 € exkl. MwSt pro Client. Diese Lizenz enthält ein ein-Jahres-Support (McAfee Gold Software Support). Für die Folgejahre belaufen sich die Kosten für die Wartung derzeit auf 18,53 € exkl. MwSt pro Jahr. (Vgl. SPP 2017) Nach der Analyse kann festgehalten werden, dass es bei etwa 336 Rechnern möglich wäre, McAfee Application Control zu installieren. Somit lägen die Anschaffungskosten bei 25.200 €, und die jährlichen Folgekosten bei etwa 6.226 €.

Für McAfee VirusScan Enterprise wird bereits der McAfee ePolicy Orchestrator am Server verwendet. Dieser kann ebenso für McAfee Application Control eingesetzt werden, daher sind in dieser Hinsicht keine weiteren Server-Kosten zu erwarten.

Da die Infrastruktur für sowohl McAfee Application Control als auch Netzwerksegmentierung bereits gegeben ist, fallen keine zusätzlichen Hardwarekosten an.

4 Einsatz von McAfee Application Control für EOL-OS in den Tirol Kliniken

Gerade bei sensiblen Klinikumgebungen ist es besonders wichtig, aktive Lösungen für die Gewährleistung der IT-Sicherheit zu implementieren. Der Schutz von Patientendaten unterliegt auf der ganzen Welt strengen Sicherheitsvorschriften und es gibt – wie bereits im Kapitel Grundlagen beschrieben – hohe Standards, denen medizintechnische Systeme unterworfen sind. Die Methode Application Control bietet eine sichere Möglichkeit, IT-Systeme und Geräte vor schädlicher Software zu schützen. Aufgrund der vorhandenen EOL-OS Clients und Supported OS Clients ohne Updates (siehe Punkt 3.2.2) in den Tirol Kliniken, überlegt die IT-Abteilung daher, McAfee Application Control für den Schutz der EOL-OS Clients einzusetzen, weswegen in diesem Kapitel besonderer Fokus auf diese Schutzmaßnahme gelegt werden soll.

Die verschiedensten Hersteller bieten Whitelisting-Programme an (Kaspersky, McAfee, Symantec, …). Da die Tirol Kliniken bereits das Antivirus-Programm von McAfee im Einsatz haben, und auch die Serverinfrastruktur in dieser Hinsicht schon existiert, wurde bei der Auswahl des Application Control Programms zu Gunsten dieses Herstellers entschieden. Das restliche Kapitel nimmt daher Bezug auf McAfee Application Control 6.1.3.443 (Solidcore Client).

4.1 Whitelisting

Wie bereits in Kapitel 2.4 kurz angerissen, stellt Application Control (Whitelisting) die genau umgekehrte Variante des Blacklisting dar: anstatt die möglichen Signaturen von Viren und Malware zu sammeln (die „nicht erlaubten“ Signaturen) und aktuell zu halten, was inzwischen durch die rasant ansteigende Zahl an verschiedenen Signaturen fast unmöglich geworden ist, werden die erlaubten Signaturen von den Programmen, die installiert werden dürfen, gesammelt. Ist die Signatur eines Programmes nicht erlaubt, so wird es nicht zur Installation zugelassen – das Prinzip der standardmäßigen Ablehnung („deny by default“). (Vgl. König 2015)

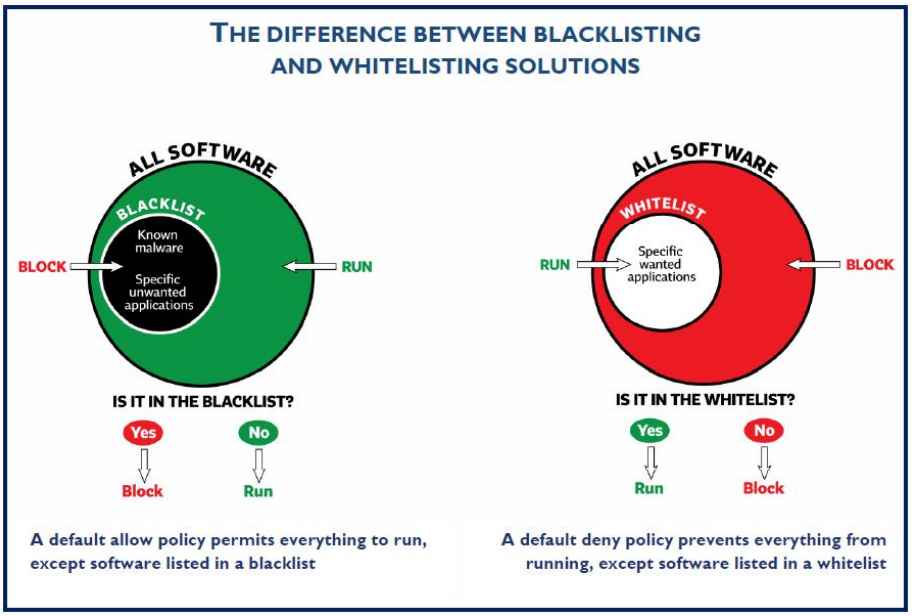

Abbildung 4-1: Blacklisting vs Whitelisting (Quelle: Dennis Technology Labs 2012)

Whitelisting ist im Vergleich zu Blacklisting um vieles schneller – anstatt nach einer der vielen Hundertausenden von Gefahren zu suchen, muss nur die überschaubare Liste der zugelassenen Programme durchforstet werden. Gerade deswegen bedeutet diese Methode natürlich eine ungemein höhere Einschränkung für die User (es werden potentiell im ersten Moment Programme oder Seiten geblockt, die der User zuvor schon jahrelang ohne Probleme genutzt hat), für die IT jedoch ist es (momentan) eine der sichersten Methoden, unzulässige Installationen zu verhindern. Whitelisting sollte jedoch keinesfalls als Standalone-Lösung gesehen werden, denn es ist kein Ersatz für eine traditionelle Blacklist. (Vgl. König 2015 und Robb 2014)

Um Whitelisting bei Clients effizient einzusetzen, müssen zwei Herausforderungen gemeistert werden: einerseits muss die Lösung die notwendigen Änderungsmechanismen unterstützen; andererseits muss sichergestellt werden, dass der Client geeignet für Whitelisting ist. Ein Client, der als COE bzw. SOE (standardisierte Umgebung in einem Unternehmen: Einsatz von gleicher Hardware, Betriebssystem, Applikationen etc.) genutzt/aufgesetzt wird, ist üblicherweise gut für diese Lösung geeignet, solange der User keine besonderen Admin-Rechte benötigt und nur Standard-Software verwendet. Sobald der User Admin-Rechte benötigt, ist Whitelisting vermutlich keine passende Lösung. Auch bei Clients, bei denen die Charakteristika von COE/SOE oder fixen funktionalen Umgebungen abweichen, könnte Whitelisting schwierig werden, da es einen großen Aufwand benötigt, um bei diesen System Whitelisting sinnvoll und effizient einzusetzen. (Vgl. Best Practices 5)

4.2 Programmbeschreibung

Im Folgenden sollen die Charakteristika und die Modi des Programms kurz beschrieben werden (Zusammengefasst nach dem Best Practices Guide von McAfee für Application Control).

4.2.1 Charakteristika

Die wohl wichtigsten Charakteristika des McAfee Application Controls sind die *Inventory* und die *Whitelist*.

Die *Inventory* besteht sowohl aus einer Liste von Applikationen, die auf einem bestimmten Client, oder Endpoint das Recht haben ausgeführt zu werden, als auch aus den Dateien auf dem Endpoint, die nicht die Erlaubnis haben ausgeführt zu werden. Die *Whitelist* ist dabei der Teil der *inventory*, der die Applikationen enthält, die ausgeführt werden dürfen und auch jene Applikationen enthält, die mittels anderer Methoden (wie Speicherort, Dateieigenschaften, Prüfsumme oder Zertifikat) erlaubt sind.

Die *Whitelist* wird jeweils vom Endpoint selbst abgeleitet. So kann diese binnen weniger Minuten erstellt werden, und so auch eher unbekannte Programme oder nicht-Standard-Versionen von Programmen erkennen (eine andere Methode wäre eine zentrale Whitelist zu erstellen, in der jede mögliche autorisierte Applikation aufgenommen wird; so werden aber oft unbekanntere Programme oder Versionen außen vor gelassen.). Um sicherzustellen, dass die Daten vom Endpoint auch tatsächlich sicher sind, werden die Details jeder Endpoint inventory an den ePolicy Orchestrator (ePO) Server weitergeleitet, wo McAfee GTI[3] einen *trust score* für jede Applikation oder binäre Datei zur Verfügung stellt. So können die vertrauenswürdigen Daten herausgefiltert werden.

Da sich in den meisten Umgebungen Applikationen, DLLs, Skripts usw. ständig ändern (durch Updates, Upgrades, Patches etc.), kann eine *dynamische Whitelist* die Wartung und Kontrolle erheblich erleichtern. Durch verschiedene Methoden wie Installers[4], Publishers[5], Updaters[6] oder trusted users wird diese dynamische Whitelist ermöglicht.

Application Control bietet unter anderem viele Speicherschutzfunktionen (*memory protection*), um Zero Day Attacken zu verhindern. Mithilfe dieser Funktionen können die folgenden zwei Exploits verhindert werden:

---

[3] Der McAfee Global Threat Intelligence (GTI) ist ein umfassender, real-time, cloudbasierter Multivektor-Service, mithilfe dessen die McAfee Produkte die Kunden gegenüber bekannten und aufkommenden Bedrohungen schützen können.
[4] Prozesse, die Teil der existierenden Inventory sind und autorisiert sind, an der Whitelist Änderungen vorzunehmen.
[5] X.509 Zertifikate, denen von der Organisation vertraut wird. Diese müssen nicht auf der Inventory sein, sind aber autorisiert auszuführen.
[6] Applikationen, die dazu verwendet werden, Software auf einem Endpoint zu installieren; sie haben sowohl das Recht auszuführen, als auch Änderungen an der Whitelist vorzunehmen.

- Buffer overflow gefolgt von *direct code execution*
- Buffer overflow gefolgt von *indirect code execution*, das *return oriented programming* verwendet

Zum Schutz vor diesen beiden Exploits verwendet Application Control vier einfache Speicherschutzfunktionen:

- CASP (Critical Address Space Protection) bietet 32bit-Endpoints Schutz vor ausgeführtem Code von non-code Bereichen im Speicher
- NX (No Execute) verwendet DEP (Data Execution Prevention von Windows), um die Ausführung von code aus non-executable Bereichen des Speichers zu verhindern. Diese Funktion ist exklusiv für 64bit-Systeme vorgesehen.
- VASR (Virtual Address Space Randomization) ergänzt und verbessert die Windows ASLR (Address Space Layout Randomization)-Technik. VASR schützt somit auch Endgeräte, die ASLR nicht unterstützen.
- Die Forced DLL Relocation erzwingt die Verschiebung von DLL Dateien, die von Windows ASLR absichtlich nicht zufällig angeordnet werden.

Das Programm enthält weiters einige selbstprotektionistische Maßnahmen. Unter anderem kann das Programm nicht deinstalliert werden, solange es im *enabled*-Modus (siehe Punkt 4.2.2) ist; die Inventory-Datei ist vor Modifikationen geschützt (sobald sie außerhalb des Application Controls verändert wird, wird ein *inventory corrupted* Event erstellt und an ePO weitergeleitet etc.

4.2.2 Modi

Das Programm bietet vier verschiedene Modi, in denen es betrieben werden kann, und zwischen denen gewechselt werden kann.

Disabled-Modus

In diesem Modus hat das Programm keinerlei Einfluss auf den Client, da der Filtertreiber und die Kernel-Komponenten nicht geladen sind und der Schutz nicht aktiv ist. In diesem Modus befindet sich das Programm, wenn es installiert wird und bevor es konfiguriert wird. Üblicherweise wird das Programm, nachdem es in einen anderen Modus umgeschalten wurde, dann nicht mehr in diesen Modus gesetzt, da in diesem Fall der Client auf jegliche Art und Weise geändert werden kann, die Inventory des Programms aber nicht up-to-date bleibt.

Enabled-Modus

Im Enabled-Modus ist das Programm aktiv; Veränderungen/Ausführungen werden nur durch die autorisierten Methoden erlaubt. Dieser Modus wird verwendet, nachdem die Policy entwickelt und getestet wurde. Durch Selbstautorisierung können User normalerweise geblockte Aktivität autorisieren (falls aktiviert).

Observe-Modus

Dieser Modus erlaubt Veränderungen, z.B. in der Inventory, wie in der Policy angegeben und dient auch dazu Veränderungen, die unter der aktuell genutzten Policy nicht erlaubt sind, zu verstehen bzw. analysieren. Diese Aktivitäten werden nicht geblockt, sondern erlaubt und zusätzliche Informationen werden dazu gesammelt. Diese Beobachtungen werden anschließend an den ePO gesendet und dort verarbeitet. Dadurch erhält man Empfehlungen, die eventuell in der Policy implementiert werden können.

Update-Modus

In diesem Modus ist Application Control aktiv, erlaubt aber die Durchführung von Produktupgrades oder –deinstallationen.

4.2.3 Auswahl und Anpassung der Policys

McAfee Application Control bietet mehrere Default-Policys an, die ausgewählt und angepasst werden können.

Product	Category	Description
Solidcore 6.1.0: Application Control	Application Control Options (Windows)	This policy is used to define self-approval, end user notifications and in rare cases to enable or disable specific features.
	Application Control Rules (Windows)	This policy defines authorised change mechanisms, exceptions, event and observation filters, and manual additions and subtractions from the whitelist for Windows endpoints.
	Application Control Rules (Unix)	This policy defines similar functionality for Unix endpoints.

Abbildung 4-2: Überblick über die Policys für Application Control (Quelle: Best Practices 2017)

Durch die richtige Auswahl und Anpassung der Policy kann die notwendige Testzeit und zusätzliche Konfiguration so weit als möglich verringert werden.

Die Konfiguration wird dabei komplett im ePO vorgenommen.

4.3 Vorgeschlagene Konfiguration in den Tirol Kliniken

In den Tirol Kliniken finden verschiedene Richtlinien Anwendung. Zusätzlich zu den Standard-Richtlinien von McAfee (Application Control Rules und Application Control Options für Windows) wurden in den Tirol Kliniken auch individuelle Richtlinien erstellt.

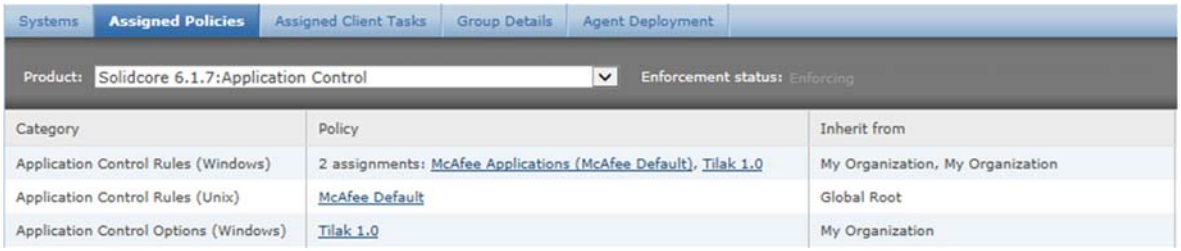

Abbildung 4-3: zugeteilte Policys in den Tirol Kliniken (Quelle: ePO)

Da in den verwendeten Standard-Richtlinien von McAfee bereits die Applikationen von McAfee erlaubt wurden, können diese in den individuell erstellten Richtlinien vernachlässigt werden.

Tilak[7] 1.0 (Application Control Options)

Über diese Policy ist es möglich, das Self Approval zu aktivieren und die dafür notwendigen Meldungen individuell anzupassen. Ebenso könnten spezielle Features, wie Memory protection oder Package Control (Deinstallation), eingestellt werden, allerdings empfiehlt McAfee dies über einen Client-Task zu definieren, was in den Tirol Kliniken auch so vorgenommen wurde.

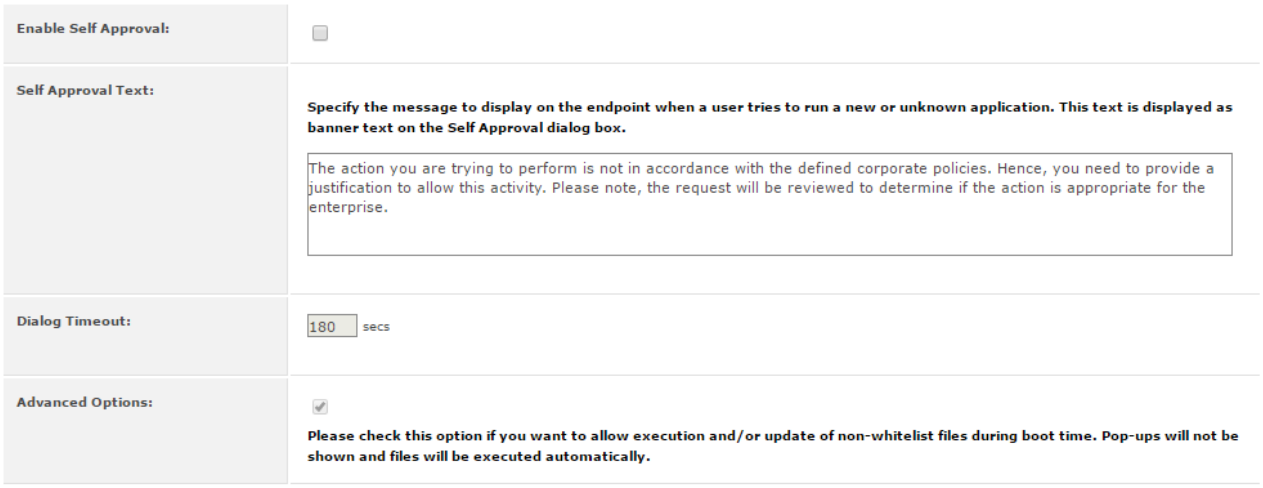

Abbildung 4-4: Enable Self Approval (Quelle: ePO)

[77] Bis zum Jahre 2015 trugen die Tirol Kliniken noch den Namen Tiroler Landeskrankenanstalten (Abkürzung: Tilak), weswegen diese Abkürzung hausintern noch oft auftritt.

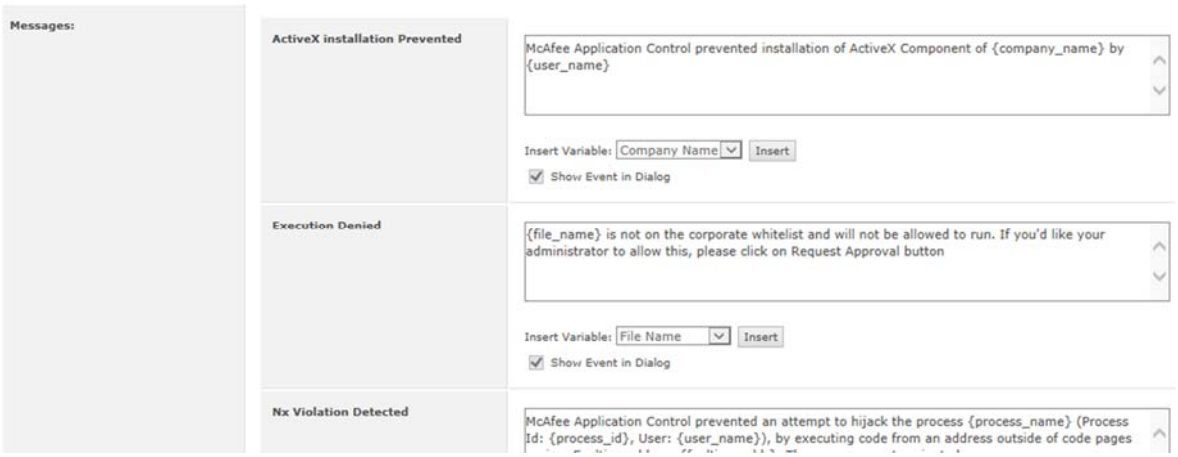

Abbildung 4-5: End User Notifications (Quelle: ePO)

Tilak 1.0 (Application Control Rules)

Mithilfe dieser Richtlinie kann die Whitelist um weitere ausführbare Dateien erweitert werden (dynamische Whitelist, siehe Punkt 4.2.1).

In der Tilak-Richtline wurden folgende Rule groups erstellt:

Abbildung 4-6: Übersicht Rule Groups der Richtlinie Tilak1.0 (Quelle: ePO)

Hier handelt es sich überwiegend um interne Programme der Tirol Kliniken.

In den folgenden Screenshots werden beispielhaft die verschiedenen Methoden einer dynamischen Whitelist anhand der Richtlinie Tilak 1.0 dargestellt:

Abbildung 4-7: Trusted Directory der Tilak-Richtlinie (Quelle: ePO)

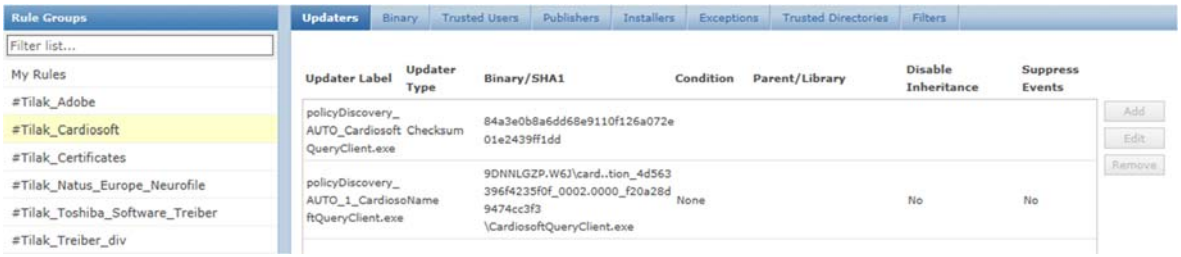

Abbildung 4-8: Updater der Tilak-Richtlinie (Quelle: ePO)

Abbildung 4-9: Publisher der Tilak-Richtlinie (Quelle: ePO)

Abbildung 4-10: Installer der Tilak-Richtlinie (Quelle: ePO)

In den Tirol Kliniken wurde vorgeschlagen, nur diejenigen Programme über die globale Richtlinie zu erlauben, die auch tatsächlich auf allen bzw. den meisten betroffenen Clients benötigt werden. Bei Programmen, bzw. ausführbaren Dateien, die nur auf vereinzelten Rechnern zum Zug kommen müssen, wird dies am einzelnen System (über den ePO) konfiguriert.

Da bislang nur einige Rechner testweise mit dem Application Control ausgestattet wurden, und noch kein derartiger Fall auftrat, gibt es hierzu kein Beispiel.

4.4 Programm zur Vereinfachung der Installation

Das folgende vom Autor geschriebene Programm soll die Installation von McAfee-Produkten auf Geräten außerhalb der Domäne vereinfachen.

Mit diesem Programm ist es möglich, den McAfee Agent mit Virus Scan Enterprise oder Application Control zu installieren. Des Weiteren können Registry Einträge gesetzt und

somit die Windows Updates eingeschalten werden, damit der interne WSUS der Tirol Kliniken verwendet wird.

Hierfür wurde das Programm in zwei Varianten geschrieben.

- McAfee_Setup-XP für Clients ab Windows 2000 (.net 3.0)
- McAfee_Setup-W7 für Clients ab Windows Vista (.net 4.5)

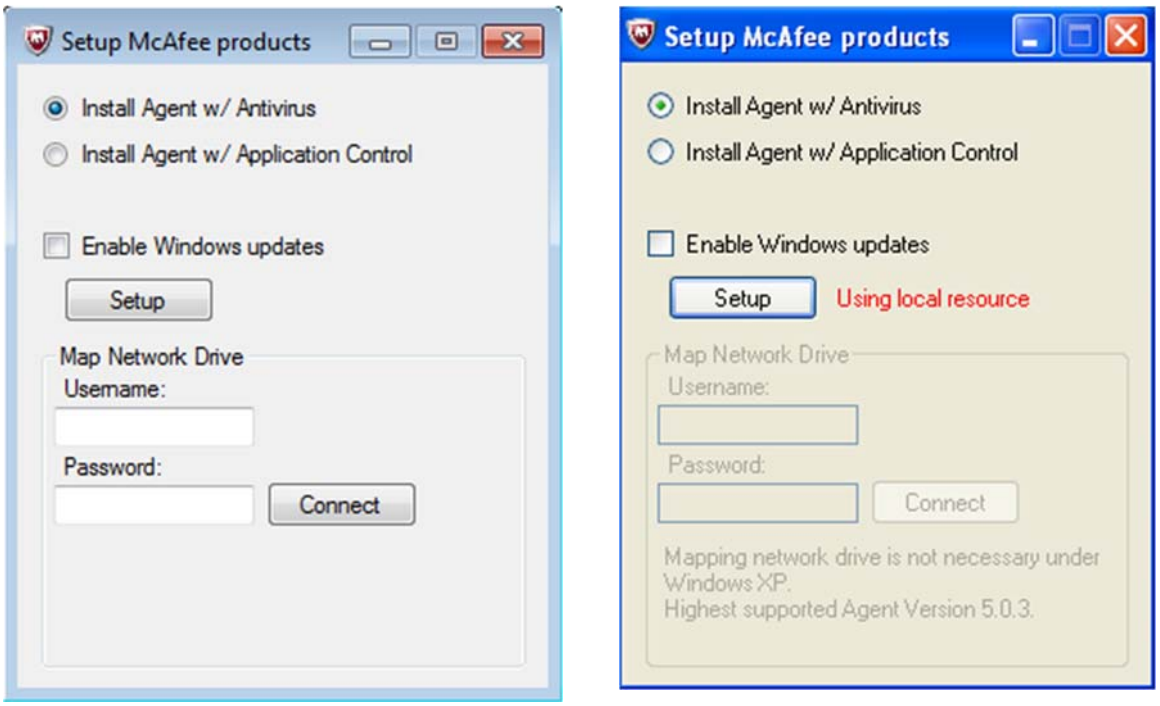

Abbildung 4-11: McAfee_Setup-W7 (links) und McAfee_Setup-XP (rechts)

Das ursprüngliche Programm wurde in C# mit .net 4.5 programmiert. Schnell stellte sich jedoch heraus, dass die eingesetzte .net Version nicht unter Windows XP lief. Ein Versuch, die .net Framework Version auf 3.0 zu ändern, führte dazu, dass die Klassen zum Verbinden eines Netzlaufwerks nicht mehr funktionierten. Da dies für Windows 2000 bzw. XP Clients nicht relevant ist, wurde diese Funktion in der XP Version des Programms weggelassen.

Programmbeschreibung McAfee_Setup-W7:

Beim Start des Programms wird überprüft, ob die Windows Version gleich 5 ist (Windows 2000 bis XP). Sollte dies der Fall sein und sich im gleichen Verzeichnis auch die Windows XP Version des Programms befinden, so wird diese anstatt der Windows 7-Version gestartet. So soll sichergestellt werden, dass, auch wenn auf den älteren Rechnern eine höhere .net-Version installiert ist (und daher die Windows 7-Version des Programmes funktionieren würde), die richtige Version des Programmes für XP geöffnet und somit auch die richtige Installationsdatei für den McAfee Agent verwendet wird.

Im Programm wurde die Installationsdatei für den McAfee Agent 5.0.5 integriert. Da zur Installation aber immer die neueste Agent-Version verwendet werden soll, muss man sich zuerst mit dem Netzlaufwerk, auf dem sich das Setup befindet, verbinden. Sollte die Verbindung zum Netzlaufwerk nicht funktionieren (falscher Benutzername oder Passwort bzw. aus einem anderen Grund), so wird man durch ein Informationsfenster aufgefordert durch Drücken der Taste *OK* die Zugangsdaten erneut einzugeben oder mittels der Taste *Abbrechen* die Installation des McAfee Agents mit der in das Programm integrierten Installationsdatei fortzusetzen.

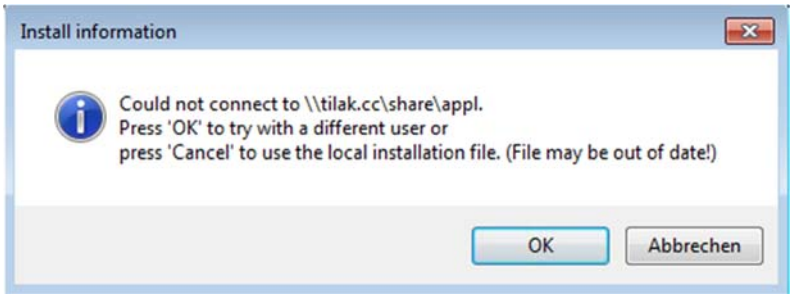

Abbildung 4-12: Informationsfenster nach nicht erfolgreicher Verbindung mit dem Netzwerklaufwerk

Hierzu wird zusätzlich die Meldung *Using local resource (File may be out of date!)* angezeigt. Konnte man sich mit dem Netzlaufwerk verbinden, so wird die neueste Installationsdatei des McAfee Agents vom Laufwerk verwendet. Nach diesem Schritt wird der Setup-Button aktiv gesetzt.

Mittels Radiobuttons kann ausgewählt werden, ob man den Agent mit Antivirus oder mit Application Control installieren möchte. Mit dem Button *Setup* startet die Installation des Agents. Die Installationen von Antivirus bzw. Application Control werden jedoch nicht über dieses Programm realisiert, sondern werden mittels ePO installiert.

Bei der Auswahl *Install Agent w/ Antivirus* wird nur der Agent im Hintergrund (silent) installiert. Virus Scan Enterprise wird dann vom ePO nachinstalliert. Bei der Auswahl *Install Agent w/ Application Control* wird der Agent wiederum silent installiert und zusätzlich das customprops1 auf den Wert *Applicationcontrol* gesetzt. Dies hat zur Folge, dass sich der gerade installierte Agent mit dem tag *Applicationcontrol* am ePO meldet, wodurch dieser dann das Produkt Application Control am Client nachinstalliert.

Mit der Checkbox *Enable Windows Updates* werden die oben erwähnten Registry-Werte gesetzt.

Programmbeschreibung McAfee_Setup-XP

Im Programm wurde die Installationsdatei für den McAfee Agent 5.0.3 integriert.

Beim Start des Programms wird überprüft, ob die Windows Version größer als 5 ist (Windows Vista und neuer). Sollte dies der Fall sein und sich im gleichen Verzeichnis auch die Windows 7 Version des Programms befinden, so wird diese anstatt der XP Version gestartet. Dies dient wiederum dazu, dass der korrekte Agent installiert wird.

In der XP-Version wurde die Funktion zum Verbinden mit dem Netzlaufwerk weggelassen, da diese mit der .net Version 3.0 nicht kompatibel ist. Da für Windows XP der höchste unterstützte Agent die Version 5.0.3 ist, wurde dieser in das Programm integriert. Somit muss am Netzlaufwerk nicht der aktuellste Agent abgerufen werden und es wird daher nur die in das Programm integrierte Installationsdatei verwendet.

4.5 Herausforderungen und aufgetretene Probleme

Bislang befinden sich die Tirol Kliniken immer noch in der Testphase und es wurden noch nicht viele EOL-OS Clients auf die eingesetzten Schutzmaßnahmen hin überprüft. Trotzdem konnten bereits einige Herausforderungen für den Einsatz von Application Control festgestellt werden. Als besonders schwierig erweist es sich, die Voraussetzungen vieler verschiedener Firmen, die medizintechnische Geräte vertreiben, unter einen Hut zu bringen. Es wurde daher ein Fragebogen an diese Firmen ausgeschickt, um möglichst schnell und effizient zu eruieren, inwiefern McAfee Application Control bei ihren Geräten eingesetzt werden könnte.

Eine weitere Schwierigkeit trat bei der Konfiguration der Clients auf. Aufgrund der Vielfalt an Systemen musste bisher jede Art von medizintechnischen Rechner (auf Basis der erstellten Policys), wie EEG, Ultraschall, usw., einzeln konfiguriert werden. Dies stellt natürlich einen erhöhten Aufwand dar, vor allem da sich die Konfiguration meist als sehr langwierig erwies.

Nach der Installation und Konfiguration des McAfee Application Control auf einem EKG-Rechner kam es zu einem verzögerten Startverhalten bei Beginn der EKG-Messung. Die Fehlersuche, bei der auch ein Techniker für McAfee zugegen war, ergab schlussendlich, dass die Aktivierung des CASP für 32bit bei einem 64bit-System zu einem solchen Fehlverhalten führte. Die Deaktivierung des CASP für 32bit konnte diesem Problem dann abhelfen.

5 Ergebnisse und Ausblick

Die ausgearbeitete Analyse unter Punkt 3 soll Unternehmen dabei unterstützen, unzureichend geschützte EOL-Rechner zu lokalisieren und einzuschätzen, was für weitere Schutzmaßnahmen noch benötigt werden. Ein Problem, das dabei in den Tirol Kliniken auftrat, war, dass die EOL-Rechner nicht wirklich managebar sind, da nicht alle am Netz angeschlossen sind. Daher ist nicht wirklich ersichtlich, wie viele EOL-Rechner noch im Unternehmen in Betrieb sind. In den Tirol Kliniken werden fast alle EOL-Rechner derzeit von den Medizintechnik- bzw. Haustechnikabteilungen gewartet (nicht von der IT-Abteilung); diese haben aber ebenfalls keine einfache Möglichkeit, diese Rechner zu verwalten. Die Techniker mussten Abteilung für Abteilung abgehen, um dies zu eruieren. Dieses Problem tritt auch sicher bei vielen anderen Firmen auf, weswegen es eine Möglichkeit benötigen würde, diese Rechner möglichst einfach zu inventarisieren und zu warten.

Es wurde festgestellt, dass das Programm Application Control nicht immer eingesetzt werden kann, um gefährdete EOL-OS Clients zu schützen, da manche Systeme (z.B. embedded systems bei Ultraschallgeräten oder ähnliches, HT wie Sensoren) dies nicht erlaubten. Stattdessen muss in diesen Fällen eine Alternative überlegt werden, die zumindest einen Grundschutz bietet (wie die Kombination aus Netzwerksegmentierung und Internet blockieren). Ein Austausch dieser Geräte kommt oft auch aus finanziellen Gründen nicht in Frage.

Es ist noch wichtig festzuhalten, dass die Überprüfung der Rechner anhand der dargestellten Analyse regelmäßig (z.B. jährlich) wiederholt werden sollte, da sich natürlich der Stand der Technik ändert, Produkte ihr Supportende erreichen, oder auch neue Produkte angeschafft werden (z.B. MT-Systeme, die nicht standardmäßig geschützt werden können). So kann sichergestellt werden, dass es nicht abermals zu einer Anhäufung ungeschützter EOL-OS Clients kommt.

McAfee Application Control wird in den Tirol Kliniken Schritt für Schritt nach Bedarf bei verschiedenen EOL-Geräten eingesetzt (vor allem bei MT-Geräten, da es hier ja vom TÜV explizit genehmigt wurde), jedoch noch nicht flächendeckend bei allen. Die Verbesserung des Schutzes von EOL-Rechnern ist in den Tirol Kliniken daher noch nicht abgeschlossen; die EOL-Rechner, die noch übrig sind, wurden in der Zwischenzeit entweder vom Netz genommen, oder werden nur (!) durch die Corporate Firewall geschützt, was keine zufriedenstellende Lösung darstellt.

Das selbstgeschriebene Programm zur Unterstützung der Installation von McAfee Application Control wurde in .net3.0 (ausführbar auf Windows XP SP 3) entwickelt. Um sicherzustellen, dass dieses Programm überall läuft, wäre es eine Möglichkeit, dieses in C zu programmieren oder als VBScript zu realisieren.

Grundsätzlich bleibt noch zu sagen, dass die ständige Weiterentwicklung im Software-Bereich es natürlich erschwert, Rechner mit EOL-OS – besonders im klinischen Bereich – zu eliminieren, da auch irgendwann der Support für die eingesetzten Schutzmaßnahmen endet. Im Gegensatz dazu stehen der enorme Aufwand und die schleppende Zertifizierung für die MT-Hersteller, deren Weiterentwicklung mitunter nicht so schnell fortschreitet. Dies erklärt die Diskrepanz zwischen den Betriebssystemen, die noch gewartet werden, und dem Stand der Computertechnik der MT-Geräte. Daher ist es umso wichtiger, dass ein Unternehmen Wert darauf legt, die noch vorhandenen EOL-Rechner rechtzeitig und ordentlich zu schützen.

Aus aktuellem Anlass muss auch noch einmal unterstrichen werden, wie wichtig die Sicherheit der EOL-Clients und die regelmäßige Aktualisierung der Betriebssysteme ist: Die WannaCry-Attacke am Wochenende des 12. Mai 2017, von der mehr als 200.000 Ziele in über 150 Länder betroffen waren, zielte auf eine Sicherheitslücke von Microsoft ab, für die erst im März ein Patch zur Verfügung gestellt worden war; allerdings erst ab Windows Vista, also den momentan unterstützten Betriebssystemen. Die hohe Anzahl der betroffenen Rechner ist vor allem auch darauf zurückzuführen, dass die Updates von Windows nicht regelmäßig bzw. automatisch von den Usern/IT-Abteilungen installiert werden. Für die Betriebssysteme Windows XP und Windows Server 2003 wurde erst nach Beginn der Attacke noch ein Patch nachgereicht, obwohl bei diesen EOL-Betriebssystemen der Support bereits vor Jahren eingestellt wurde. (Vgl. Heise und BBC)

Literatur

Eckert 2012 — Eckert, Claudia (2012[7]): IT-Sicherheit. Konzepte – Verfahren – Protokolle. München: Oldenbourg Verlag.

Kappes 2007 — Kappes, Martin (2007): Netzwerk- und Datensicherheit. Eine praktische Einführung. Wiesbaden: B.G. Teubner Verlag

Kerner 1992 — Kerner, Helmut (1992): Rechnernetze nach OSI. Bonn, München, Paris: Addison Wesley.

Kersten et al. 2013 — Kersten, Heinrich / Reuter, Jürgen / Schröder, Klaus-Werner (2013[4]): IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Wiesbaden: Springer Fachmedien.

Pfleeger & Pfleeger 2007 — Pfleeger, Charles P / Pfleeger Shari Lawrence (2007[4]): Security in Computing. New Jersey: Prentice Hall, Pearson Education Inc.

Pohlmann & Blumberg 2004 — Pohlmann, Norbert / Blumberg, Hartmut (2004): Der IT-Sicherheitsleitfaden. Das Pflichtenheft zur Implementierung von IT-Sicherheitsstandards im Unternehmen. Bonn: mitp Verlag.

Atencio Psille & Eschweiler — Atencio Psille, Daniel E. / Eschweiler, Jörg (2006): Security@Work. Pragmatische Konzeption und Implementierung von IT-Sicherheit mit Lösungsbeispielen auf Open-Source-Basis. Berlin, Heidelberg: Springer-Verlag.

Schneider 2012 — Schneider, Uwe (Hrsg.) (2012[7]): Taschenbuch der Informatik. München: Carl Hanser Verlag

Müller 2014 — Müller, Klaus-Rainer (2014[5]): IT-Sicherheit mit System. Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – sichere Anwendungen – Standards und Practices. Wiesbaden: Springer Vieweg.

Artikel

Jendrian 2014 — Jendrian, Kai (2014): Der Standard ISO/IEC 27001:2013. In: Datenschutz und Datensicherheit - DuD. August 2014, Volume 38, Issue 8, pp 552-557.

Eikenberg & Schulz 2017 — Eikenberg Ronald / Schulz Hajo (2017). Windows Update im Griff. Warum regelmäßige Patches so wichtig sind. In: c’t

03/2017, p 98.

Rechtstexte und Normen

DSG — Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), Fassung vom 28.05.2017, Bundesrepublik Österreich.

ISO 27001:2013 — Informationstechnologie — Sicherheitstechnik — Informationssicherheits-Managementsysteme — Anforderungen (ISO/IEC 27001:2013 + Cor.1:2014). Ausgabe: 01.09.2015.

MPG — Bundesgesetz betreffend Medizinprodukte (Medizinproduktegesetz - MPG), Fassung vom 01.05.2016, Bundesrepublik Österreich.

MPBV — Verordnung der Bundesministerin für Gesundheit, Familie und Jugend über das Errichten, Betreiben, Anwenden und Instandhalten von Medizinprodukten in Einrichtungen des Gesundheitswesens (Medizinproduktebetreiberverordnung - MPBV), Fassung vom 01.05.2016, Bundesrepublik Österreich.

Internetquellen

ACOnet — Verfügbar unter:
https://www.aco.net/
Zuletzt abgerufen am: 16.02.2017

AV-Test — AV-Test: The Independent IT-Security Institute. Security Report 2015/16. Magdeburg (2016).
Verfügbar unter:
https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Sicherheitsreport_2015-2016.pdf
Zuletzt abgerufen am: 05.02.2017

BBC — Ransomware cyber-attack threat escalating – Europol. BBC News. 14.05.2017
Verfügbar unter:
http://www.bbc.com/news/technology-39913630
Zuletzt abgerufen am: 20.05.2017

Best Practices — Application Control for Desktops Best Practices Guide 1.0. Application Control / Change Control Best Practices Guide
Produktdokumentation ID: PD24662; Zuletzt geändert am: 2/1/2017
Verfügbar unter:
https://kc.mcafee.com/corporate/index?page=content&id=PD2

4662&actp=null&viewlocale=en_US&showDraft=false&platinum_status=false&locale=de_DE
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24662/en_US/AppCtrl_BestPractices_Guide.pdf
Zuletzt abgerufen am: 14.05.2017

Cade 2015 — Cade Curtis. Understanding Heuristic-based Scanning vs. Sandboxing. Opswat (2015)
Verfügbar unter:
https://www.opswat.com/blog/understanding-heuristic-based-scanning-vs-sandboxing
Zuletzt abgerufen am: 14.05.2017

CERT 2017 — GovCERT Austria. Internet-Sicherheit Österreich 2016. Bericht. Wien (2017).
Verfügbar unter:
https://cert.at/downloads/reports/jahresbericht-2016.html
Zuletzt abgerufen am: 18.02.2017

CVE 2016 — Özkan Serkan. CVE Details. The ultimate security vulnerability datasource.
Verfügbar unter:
https://www.cvedetails.com
Zuletzt abgerufen am: 05.02.2017

Datenschutz I — Berliner Beauftragte für Datenschutz und Informationsfreiheit. Verfügbarkeit, Integrität, Vertraulichkeit, Authentizität. (2008)
Verfügbar unter:
http://www.datenschutz-berlin.de/content/technik/begriffsbestimmungen/verfuegbarkeit-integritaet-vertraulichkeit-authentizitaet
Zuletzt abgerufen am: 12.05.2017

Dennis Technology Labs 2012 — Dennis Technology Labs. Application Control Comparison. Report November 2012.
Verfügbar unter:
http://dennistechnologylabs.com/reports/s/app-control/kaspersky/DTL_2012_KL-AppCtl1.2.pdf
Zuletzt abgerufen am: 15.04.2017

FAQ — Bundesamt für Sicherheit in der Informationstechnik. FAQ.

Verfügbar unter:
https://www.bsi.bund.de/DE/Service/FAQ/faq_node.html
Zuletzt abgerufen am: 14.05.2017

GÉANT — Verfügbar unter:
http://www.geant.org/
Zuletzt abgerufen am: 16.02.2017

Heise — Briegleb Volker. WannaCry: Was wir bisher über die Ransomware-Attacke wissen. Heise online. 13.05.2017
Verfügbar unter:
https://www.heise.de/newsticker/meldung/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html
Zuletzt abgerufen am: 20.05.2017

IT-Grundschutz 1 — Bundesamt für Sicherheit in der Informationstechnik. IT-Grundschutzkataloge. Kapitel 1. Bonn.
Verfügbar unter:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/allgemein/einstieg/01001.html
Zuletzt abgerufen am: 01.02.2016

IOCTA — Europol. IOCTA 2016. Internet Organised Crime Threat Assessment. The Hague (2016).
Verfügbar unter:
https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016
Zuletzt abgerufen am: 18.02.2016

Kumar 2009 — Kumar Vikram. What do P2P Applications do and How to block Peer to Peer Applications (P2P) using Symantec Endpoint Protection? Symantec (2009).
Verfügbar unter:
https://www.symantec.com/connect/articles/what-do-p2p-applications-do-and-how-block-peer-peer-applications-p2p-using-symantec-endpoin
Zuletzt abgerufen am: 11.02.2017

Khalimonenko et al 2016 — Khalimonenko Alexander / Strohschneider Jens / Kupreev Oleg. DDoS-Attacken im dritten Quartal 2016. Quartalsreport Malware (Kaspersky Lab), 31.10.2016, 08:57.
Verfügbar unter:
https://de.securelist.com/analysis/quartalsreport-malware/72097/kaspersky-ddos-intelligence-report-for-q3-

2016/
Zuletzt abgerufen am: 18.02.2017

Khalimonenko et al 2017 — Khalimonenko Alexander / Strohschneider Jens / Kupreev Oleg. DDoS-Attacken im vierten Quartal 2016. Quartalsreport Malware (Kaspersky Lab), 02.02.2017, 11:00.
Verfügbar unter:
https://de.securelist.com/analysis/quartalsreport-malware/72359/ddos-attacks-in-q4-2016/
Zuletzt abgerufen am: 18.02.2017

König 2015 — König Jürgen. Proaktive IT-Sicherheit durch Application-Whitelisting. funkschau, 13.03.2015.
Verfügbar unter:
http://www.funkschau.de/datacenter/artikel/117939/
Zuletzt abgerufen am: 01.04.2017

NexThink — Verfügbar unter:
https://doc.nexthink.com/Documentation/Nexthink/latest/ProductOverview
Zuletzt abgerufen am: 28.05.2017

Pressemitteilung Kaspersky Lab — Kaspersky Lab / Schafroth Florian (2017). Unsichtbare Angriffe: Im Speicher versteckte Malware greift Unternehmen in 40 Ländern an. Pressemitteilung, 08.02.2017.
Verfügbar unter:
http://newsroom.kaspersky.eu/de/texte/detail/article/unsichtbare-angriffe-im-speicher-versteckte-malware-greift-unternehmen-in-40-laendern-an
Zuletzt abgerufen am: 11.02.2017

Reed 2003 — Reed Damon. Applying the OSI Seven Layer Network Model To Information Security. SANS Institute (2003).
Verfügbar unter:
https://www.sans.org/reading-room/whitepapers/protocols/applying-osi-layer-network-model-information-security-1309
Zuletzt abgerufen am: 14.05.2017

Robb 2017 — Robb Drew. Whitelisting: Why and How It Works. eSecurity Planet, 24.09.2014.
Verfügbar unter:
http://www.esecurityplanet.com/malware/whitelisting-why-and-how-it-works.html
Zuletzt abgerufen am: 01.04.2017

Statistik Austria — Statitik Austria – Krankenstandstage. Verfügbar unter: http://www.statistik.at/web_de/statistiken/menschen_und_gesellschaft/gesundheit/gesundheitszustand/krankenstandstage/index.html Zuletzt abgerufen am: 02.05.2017

Nachschlagewerke:

Duden Universal — Duden – Deutsches Universalwörterbuch (^{6}2006). Mannheim: Dudenverlag.

ITWissen — http://www.itwissen.info

Kaspersky-Lexikon — https://de.securelist.com/lexikon/

Techstories — https://wiki.techstories.de

Korrespondenz

SPP 2017 — SPP Handelsges. m.b.H. Wien, 10.05.2017 an Tirol Kliniken.

TÜV 2015 — TÜV AUSTRIA SERVICES GMBH, Innsbruck, 25.08.2015 an Tirol Kliniken.

Anlagen

Anlage A. Email TÜV – McAfee Application Control

Von: [redacted]
Gesendet: Dienstag, 25. August 2015 11:51
An: [redacted]
Cc: [redacted]
Betreff: AW: Bitte um Stellungnahme bzgl. "McAfee Application Control"

Sehr geehrter Herr [redacted],
sehr geehrter [redacted]

Das "McAfee Application Control" ist laut den Unterlagen ein offizielles, zugelassenes Programm. In der Beschreibung sind auch Medizinprodukte angesprochen und dezidiert nicht ausgeschlossen. Das ist ein guter Ansatz.
Insofern müsste das Thema MP auch seitens des SW Hersteller berücksichtigt sein. Auch von Eurer Seite als IT Spezialisten wurde das SW Programm hinsichtlich der sicheren Verwendbarkeit evaluiert. Ich würde also davon ausgehen, dass mit diesem Programm grundsätzlich eine qualitative Verbesserung der „Instandhaltung“ der MP nach MPBV im Sinne der Patienten und Datensicherheit gegeben ist. Falls ein Hersteller das anders sieht, sollte er Programmierungstechnisch genau das mögliche Sicherheitsproblem identifizieren und darstellen. Eine pauschale, unbegründete Ablehnung seitens der Hersteller halte ich nicht für ausreichend und würde das eher in Richtung Verkaufsstrategie sehen. Sicherheitshalber könnte man den jeweiligen Hersteller vorab, mit der Bitte der fachlichen Begründung der Ablehnung, kontaktieren.
Für Rückfragen oder Besprechungen stehe ich gerne zur Verfügung.

Mit freundlichen Grüßen
[redacted]

TSB Tirol Kliniken
[redacted]
TÜV AUSTRIA SERVICES GMBH

Anlage B. McAfee_Setup-W7

Program.cs

```
1.  using System;
2.  using System.Diagnostics;
3.  using System.IO;
4.  using System.Windows.Forms;
5.  namespace McAfee_Setup_W7 {
6.      static class Program {
7.          static Process p = new Process();
8.          [STAThread] static void Main() {
9.              if (Environment.OSVersion.Version.Major == 5) {
10.                 FileInfo setup = new FileInfo(Path.Combine(
    AppDomain.CurrentDomain.BaseDirectory, "McAfee_Setup-WXP.exe"));
11.                 if (setup.Exists) {
12.                     Process.Start(setup.FullName);
13.                 } else {
14.                     Application.EnableVisualStyles();
15.                     Application.SetCompatibleTextRenderingDefault(false);
16.                     Application.Run(new frmMain());
17.                 }
18.             } else {
19.                 Application.EnableVisualStyles();
20.                 Application.SetCompatibleTextRenderingDefault(false);
21.                 Application.Run(new frmMain());
22.             }
23.         }
24.         public static void install(string arg, bool local) {
25.             string workdir;
26.             string file = "FramePkg.exe";
27.             if (local) {
28.                 ExtractResource(file, Properties.Resources.FramePkg); //Version 5.0.5
29.                 workdir = Path.GetTempPath();
30.             } else {
31.                 workdir = Network path to FramePkg.exe;
32.             }
33.             p.StartInfo.WorkingDirectory = workdir;
34.             p.StartInfo.FileName = file;
35.             p.StartInfo.Arguments = arg;
36.             p.Start();
37.             p.WaitForExit();
38.             if (local) {
39.                 deletefile(file);
40.             }
41.             MessageBox.Show("Installation complete");
42.         }
43.         private static void ExtractResource(string filename, byte[] resource) {
44.             File.WriteAllBytes(Path.Combine(Path.GetTempPath(), filename), resource);

45.         }
46.         private static void deletefile(string filename) {
47.             File.Delete(Path.Combine(Path.GetTempPath(), filename));
48.         }
49.     }
50. }
```

Form1.cs

```
1.  using System;
2.  using System.Windows.Forms;
3.  using IWshRuntimeLibrary;
4.  using System.Collections;
5.  using Microsoft.Win32;
6.  using System.DirectoryServices.AccountManagement;
7.  namespace McAfee_Setup_W7 {
8.      public partial class frmMain: Form {
9.              private IWshNetwork_Class network = new IWshNetwork_Class();
10.             DialogResult msgbx;
11.             public frmMain() {
12.                 InitializeComponent();
13.             }
14.             private void frmMain_Activated(object sender, EventArgs e) {
15.                 EnableSetupButton();
16.                 if (checkShares()) {
17.                     lblWarning.Text = @"Warning! There are already connections to the
    share Sharename.  ALL connections will be closed!";
18.                 } else {
19.                     lblWarning.Text = @"McAfee folder on Network folder is not
    accessible. Map network drive w/ different user.";
20.                 }
21.             }
22.             private void cmdSetup_Click(object sender, EventArgs e) {
23.                 string result = null;
24.                 bool local = false;
25.                 if (msgbx == DialogResult.Cancel) {
26.                     local = true;
27.                 } else {
28.                     local = false;
29.                 }
30.                 foreach(Control control in Controls) {
31.                     if (control is RadioButton) {
32.                         RadioButton radio = control as RadioButton;
33.                         if (radio.Checked) {
34.                             result = radio.Name;
35.                         }
36.                     }
37.                 }
38.                 Cursor.Current = Cursors.WaitCursor;
39.                 switch (result) {
40.                     case "optAV":
41.                         Program.install("/silent /install=agent", local);
42.                         break;
43.                     case "optAC":
44.                         Program.install("/silent /install=agent
    /customprops1=\"Applicationcontrol\"", local);
45.                         break;
46.                 }
47.                 Cursor.Current = Cursors.Default;
48.             }
49.             private void chkWSUS_CheckedChanged(object sender, EventArgs e) {
50.                 if (chkWSUS.Checked == true) {
51.                     string path = @"SOFTWARE\Policies\Microsoft\Windows";
52.                     RegistryKey key = Registry.LocalMachine.OpenSubKey(path, true);
53.                     key.CreateSubKey("WindowsUpdate");
54.                     key = key.OpenSubKey("WindowsUpdate", true);
55.                     key.SetValue("WUServer", Server URL, RegistryValueKind.String);
56.                     key.SetValue("WUStatusServer", Server URL,
    RegistryValueKind.String);
57.                     key = key.CreateSubKey("AU");
58.                     key.SetValue("NoAutoUpdate", 0, RegistryValueKind.DWord);
59.                     key.SetValue("AUOptions", 4, RegistryValueKind.DWord);
```

```
60.                     key.SetValue("ScheduledInstallDay", 0, RegistryValueKind.DWord);
61.                     key.SetValue("ScheduledInstallTime", 3, RegistryValueKind.DWord);
62.                     key.SetValue("UseWUServer", 1, RegistryValueKind.DWord);
63.                     key.SetValue("DetectionFrequencyEnabled", 1,
    RegistryValueKind.DWord);
64.                     key.SetValue("DetectionFrequency", 8, RegistryValueKind.DWord);
65.                     key.SetValue("AutoInstallMinorUpdates", 1,
    RegistryValueKind.DWord);
66.                     key.Close();
67.                     MessageBox.Show("Windows updates enabled");
68.                 } else {
69.                     string path = @"SOFTWARE\Policies\Microsoft\Windows";
70.                     RegistryKey key = Registry.LocalMachine.OpenSubKey(path, true);
71.                     key.DeleteSubKeyTree("WindowsUpdate");
72.                     key.Close();
73.                     MessageBox.Show("Windows updates disabled");
74.                 }
75.             }
76.             private void cmdConnect_Click(object sender, EventArgs e) {
77.                 if (checkPwd()) {
78.                     mapDrives();
79.                     EnableSetupButton();
80.                 }
81.             }
82.             private void EnableSetupButton() {
83.                 if (msgbx == DialogResult.Cancel) {
84.                     cmdSetup.Enabled = true;
85.                     lblInformation.Visible = true;
86.                 } else {
87.                     lblInformation.Visible = false;
88.                  if (System.IO.File.Exists(@"Network path to\FramePkg.exe")) {
89.                         cmdSetup.Enabled = true;
90.                     } else {
91.                         cmdSetup.Enabled = false;
92.                     }
93.                 }
94.             }
95.             private bool checkPwd() {
96.                 try {
97.                     using(PrincipalContext context = new PrincipalContext(
    ContextType.Domain, "Domain", txtUser.Text, txtPass.Text)) {
98.                         if (!context.ValidateCredentials(txtUser.Text, txtPass.Text,
    ContextOptions.Negotiate)) {
99.                             lblWarning.Visible = true;
100.                                lblCredWarning.Visible = true;
101.                                return false;
102.                            } else {
103.                                lblWarning.Visible = false;
104.                                lblCredWarning.Visible = false;
105.                            }
106.                            return true;
107.                        }
108.                    } catch (Exception e) {
109.                        if (e.HResult == -2147023570 || e.HResult == -2147016672) {
110.                            lblCredWarning.Visible = true;
111.                            return false;
112.                        }
113.                        return true;
114.                    }
115.                    private void mapDrives() {
116.                        try {
117.                            IWshCollection nwDrives = network.EnumNetworkDrives();
118.                            for (int i = 0; i < nwDrives.Count(); i += 2) {
119.                             if (nwDrives.Item(i + 1).ToString().Contains(@"\\Domain"
    )) {
```

```
120.                                     network.RemoveNetworkDrive(nwDrives.Item(i).ToStr
    ing(), true, true);
121.                                 }
122.                             }
123.                             network.MapNetworkDrive("Z:", Network folder,
    Type.Missing, Domain + txtUser.Text, txtPass.Text);
124.                                 msgbx = DialogResult.OK;
125.                             } catch (Exception) {
126.                                 msgbx = MessageBox.Show(@"Could not connect to
    Network folder." + Environment.NewLine + "Press 'OK' to try with a different user or"
     + Environment.NewLine + "press 'Cancel' to use the local installation file. (File
    may be out of date!)", "Install information", MessageBoxButtons.OKCancel,
    MessageBoxIcon.Information);
127.                             }
128.                         }
129.                         private void txtUser_KeyUp(object sender, KeyEventArgs e) {
130.                             if (e.KeyCode == Keys.Enter) {
131.                                 cmdConnect_Click(sender, e);
132.                             }
133.                         }
134.                         private void txtPass_KeyUp(object sender, KeyEventArgs e) {
135.                             if (e.KeyCode == Keys.Enter) {
136.                                 cmdConnect_Click(sender, e);
137.                             }
138.                         }
139.                         private bool checkShares() {
140.                             IWshCollection nwDrives = network.EnumNetworkDrives();
141.                             foreach(IEnumerable drive in nwDrives) {
142.                                 if (drive.ToString().Contains(@"\\Domain")) {
143.                                     return true;
144.                                 }
145.                             }
146.                             return false;
147.                         }
148.                     }
149.                 }
```

Anlage C. McAfee_Setup-WXP

Program.cs

```
1.  using System;
2.  using System.Diagnostics;
3.  using System.IO;
4.  using System.Windows.Forms;
5.  namespace McAfee_Setup_WXP {
6.      static class Program {
7.          static Process p = new Process();
8.          [STAThread] static void Main() {
9.              if (Environment.OSVersion.Version.Major > 5) {
10.                 FileIn-
    fo setup = new FileInfo(Path.Combine(AppDomain.CurrentDomain.BaseDirectory,
    "McAfee_Setup-W7.exe"));
11.                 if (setup.Exists) {
12.                     Process.Start(setup.FullName);
13.                 } else {
14.                     Application.EnableVisualStyles();
15.                     Application.SetCompatibleTextRenderingDefault(false);
16.                     Application.Run(new frmMain());
17.                 }
18.             } else {
19.                 Application.EnableVisualStyles();
20.                 Application.SetCompatibleTextRenderingDefault(false);
21.                 Application.Run(new frmMain());
22.             }
23.         }
24.         public static void install(string arg) {
25.             string file = "FramePkg.exe";
26.             ExtractResource(file, Properties.Resources.FramePkg); //Version 5.0.3
27.             p.StartInfo.WorkingDirectory = Path.GetTempPath();
28.             p.StartInfo.FileName = file;
29.             p.StartInfo.Arguments = arg;
30.             p.Start();
31.             p.WaitForExit();
32.             deletefile(file);
33.             MessageBox.Show("Installation complete");
34.         }
35.         private static void ExtractResource(string filename, byte[] resource) {
36.             File.WriteAllBytes(Path.Combine(Path.GetTempPath(), filename), resource);
37.         }
38.         private static void deletefile(string filename) {
39.             File.Delete(Path.Combine(Path.GetTempPath(), filename));
40.         }
41.     }
42. }
```

Form1.cs

```
1.  using System;
2.  using System.Windows.Forms;
3.  using System.Collections;
4.  using Microsoft.Win32;
5.  namespace McAfee_Setup_WXP {
6.      public partial class frmMain: Form {
7.          public frmMain() {
8.              InitializeComponent();
9.              lblWarning.Text = @"Mapping network drive is not necessary under Windows
    XP." + Environment.NewLine + "Highest supported Agent Version 5.0.3.";
10.         }
11.         private void cmdSetup_Click(object sender, EventArgs e) {
12.             string result = null;
13.             foreach(Control control in Controls) {
14.                 if (control is RadioButton) {
15.                     RadioButton radio = control as RadioButton;
16.                     if (radio.Checked) {
17.                         result = radio.Name;
18.                     }
19.                 }
20.             }
21.             Cursor.Current = Cursors.WaitCursor;
22.             switch (result) {
23.                 case "optAV":
24.                     Program.install("/silent /install=agent");
25.                     break;
26.                 case "optAC":
27.                     Program.install("/silent /install=agent
    /customprops1=\"Applicationcontrol\"");
28.                     break;
29.             }
30.             Cursor.Current = Cursors.Default;
31.         }
32.         private void chkWSUS_CheckedChanged(object sender, EventArgs e) {
33.             if (chkWSUS.Checked == true) {
34.                 string path = @"SOFTWARE\Policies\Microsoft\Windows";
35.                 RegistryKey key = Registry.LocalMachine.OpenSubKey(path, true);
36.                 key.CreateSubKey("WindowsUpdate");
37.                 key = key.OpenSubKey("WindowsUpdate", true);
38.                 key.SetValue("WUServer", Server URL, RegistryValueKind.String);
39.                 key.SetValue("WUStatusServer", Server URL, RegistryValueKind.String);
40.                 key = key.CreateSubKey("AU");
41.                 key.SetValue("NoAutoUpdate", 0, RegistryValueKind.DWord);
42.                 key.SetValue("AUOptions", 4, RegistryValueKind.DWord);
43.                 key.SetValue("ScheduledInstallDay", 0, RegistryValueKind.DWord);
44.                 key.SetValue("ScheduledInstallTime", 3, RegistryValueKind.DWord);
45.                 key.SetValue("UseWUServer", 1, RegistryValueKind.DWord);
46.                 key.SetValue("DetectionFrequencyEnabled", 1, RegistryValueKind.DWord);

47.                 key.SetValue("DetectionFrequency", 8, RegistryValueKind.DWord);
48.                 key.SetValue("AutoInstallMinorUpdates", 1, RegistryValueKind.DWord);
49.                 key.Close();
50.                 MessageBox.Show("Windows updates enabled");
51.             } else {
52.                 string path = @"SOFTWARE\Policies\Microsoft\Windows";
53.                 RegistryKey key = Registry.LocalMachine.OpenSubKey(path, true);
54.                 key.DeleteSubKeyTree("WindowsUpdate");
55.                 key.Close();
56.                 MessageBox.Show("Windows updates disabled");
57.             }
58.         }
59.     }
60. }
```

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Innsbruck, 29. Mai 2017

Ing. Michael Sandro Erhart