Cyberrisiken der Universität Zürich

Philip Hofmann

Othmarsingen, Aargau, CH

14-710-842

BACHELORARBEIT

eingereicht beim

Institut für Informatik

im Studiengang

Wirtschaftsinformatik

an der Universität Zürich UZH

Eingereicht am 01. Februar 2018

Diese Arbeit entstand unter Betreuung von

Prof. Dr. Lorenz Hilty

Inhaltsverzeichnis

Danksagung

An dieser Stelle möchte ich Professor Hilty danken, der es mir erlaubte, mein eigenes Thema einzubringen, und mir auch bei der Bearbeitung dieses Themas viel Freiraum liess. Danken möchte ich unter anderem auch Herrn Sacha Schweizer, dem IT-Security Officer der Universität Zürich, und Herrn Silvio Oertli, Security Experte bei SWITCH-CERT, welche sich beide die Zeit nahmen, Fragen zu beantworten. Zu guter Letzt möchte ich meinem Bruder für seine Unterstützung in dieser Sache danken, und natürlich meiner ganzen Familie für die Unterstützung während meines gesamten Bachelorstudiums.

Einleitung

In der heutigen, digital vernetzten Welt ist Informationssicherheit ein wichtiges Thema. Die Medien berichten häufig von Cyberangriffen auf Institutionen, in denen die Angriffe verschiedene Ziele verfolgten, wie die angegriffene Institution zu infiltrieren, zu sabotieren, wichtige Daten abzugreifen oder durch diese Institution später Attacken auf andere Ziele durchzuführen. Zu diesen potenziell angreifbaren und schützenswerten Institutionen zählen auch die Schweizer Hochschulen, welche aufgrund von Forschungstätigkeiten, Ausbildungspflichten und aus der Privatwirtschaft in Auftrag gegebenen Studien wertvolle Daten sammeln und generieren. Die Resultate dieser Studien und die aus den Forschungsprojekten resultierenden Technologien und Spin-off-Firmen haben einen potenziellen Einfluss auf die gesamte Schweizer Wirtschaft.

Diese Arbeit betrachtet den momentanen Stand, welche die Informationssicherheit in der Schweiz einnimmt, zeigt in diesem Zusammenhang die Verbundenheit der Hochschulen in der Schweiz zu anderen Organisationen, listet einige mögliche Cyberbedrohungen von Ausserhalb und wirft einen Blick auf die an der Universität Zürich eingesetzten Abwehrmechanismen. Danach erarbeitet diese Arbeit anhand identifizierter Anreize für potenzielle Angreifer drei mögliche Szenarien von Cyberattacken gegen die Universität Zürich, zusammen mit deren potenziellen Auswirkungen. Die Arbeit gibt abschliessend Empfehlungen ab, welche die Risiken von gewissen Cyberbedrohungen senken könnten. Da sich professionelle Angestellte der Universität Zürich bereits mit diesem Thema beschäftigen, nimmt der Autor hier eine Beobachterposition ein.

Kapitel 1

Bedrohungslage Schweiz

1.1 Informationssicherheit Schweiz

Um einen Überblick über die Lage der Informationssicherheit in der Schweiz zu erhalten, betrachten wir die möglichen offiziellen Anlaufstellen zum Thema Cybersecurity, welche den Firmen und Hochschulen Unterstützung betreffend diesem Thema bieten können. Dann bedienen wird uns der einzigen vom Bund je in Auftrag gegebener Studie über die Informationssicherheit in Schweizer Unternehmen und ziehen dann ein paar aktuellere Reporte zurate.

Eine offizielle Anlaufstelle bezüglich Meldungen zu Cyberangriffen ist die Melde- und Analysestelle Informationssicherung MELANI, welche seit 2004 operativ tätig ist. Laut der offiziellen Homepage [1] ist MELANI ein

> Kooperationsmodell zwischen dem Eidgenössischen Finanzdepartement (EFD), vertreten durch das Informatiksteuerungsorgan des Bundes (ISB) und dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), vertreten durch den Nachrichtendienst des Bundes (NDB)[2].

Das SIB sorgt für die Umsetzung der Informations- und Kommunikationstechnologie (IKT) des Bundesrates, weshalb dann auch 2012 MELANI mit der Umsetzung der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken» beauftragt wurde. Um ihren Auftrag noch besser wahrnehmen zu können, schuf MELANIE das Swiss Governmental Computer Emergency Response Team GovCERT, welches seit 2008 operativ ist. Auf der offiziellen Homepage govcert.admin.ch wird erklärt, dass diese für die technischen Aspekte und Analyse von gemeldeten Vorfällen verantwortlich ist. MELANIE selbst veröffentlicht auch immer wieder Informationen betreffend der Informationssicherheit in der Schweiz, so aktuelle Gefahren, Ratschläge zum Schutze vor Cyberangriffen für Privatpersonen und Firmen, sowie

[1] https://www.melani.admin.ch/melani/de/home.html

[2] Zitat entnommen von https://www.melani.admin.ch/melani/de/home/ueber-melani/organisation.html

auch einen halbjährlichen Lagebericht 'Informationssicherung: Lage in der Schweiz und international', worin die beobachteten Entwicklungen, Tendenzen und Vorfälle in Bezug auf die Informationssicherheit erläutert werden, sowie auch die technische Funktionsweisen aktueller Angriffe und beleuchtet die wichtigsten Entwicklungen im Bereich der Präventation. Neben diesen offiziellen Anlaufstellen sehen wir auch die Gründung weiterer Organisationen, so wurde zum Beispiel Im Jahr 2014 wurde die Swiss Internet Security Alliance (SISA) von führenden Vertretern der Schweizer Wirtschaft gegründet, die sich für den sicheren Internet-Standort Schweiz einsetzt. Sie führt Awareness-Projekte durch und bietet unter anderem Sicherheits-Checks für Privatpersonen an.

Während Studien auf nationaler Ebene zum Thema Informationssicherheit zu dieser Zeit in anderen Ländern bereits durchgeführt wurden, fehlte eine solche bis im Jahre 2005 noch in der Schweiz. Daher wurde die Forschungsstelle für Sicherheit der ETH Zürich, das Center for Security Studies (CSS), damit beauftragt, eine solche Studie über den Stand des Schutzes sowie der Bedrohungslage im Cyberraum aus Sicht der Schweizer Wirtschaft durchzuführen. Diese wurde schliesslich im August 2006 publiziert. Dabei gibt es zu Bedenken, dass diese Studie hauptsächlich einen Einblick in die Situation des Jahres 2005 gibt. Es gibt leider in der Schweiz momentan keine aktuellere nationale Studie dieser Art, und trotzdem kann uns die Betrachtung dieser Studie eine gute Grundlage geben, wie die Situation aktuell ungefähr aussehen könnte. Diese Studie wurde seinerzeit auf Grundlage einer durchgeführten Umfrage unter Schweizer Firmen verfasst.

Im Folgenden begutachten wir ein paar interessante Punkte, die aus dieser Umfrage resultierten. Bezogen auf die Häufigkeit der Vorfälle gaben 72% der befragten Unternehmen an, im Jahre 2005 mindestens einen Vorfall in der Informationssicherheit bemerkt zu haben. Die Studie bemerkte hier, dass die Zusammensetzung der befragten Firmen nicht repräsentativ sei, bei der Anwendung des statistischen Verfahrens der Gewichtung käme man dabei auf einen Schätzwert von 63% aller schweizerischen Unternehmen, die einen Vorfall gehabt hätten. Abbildung 1.1 visualisiert die Verteilung der Angriffsmethoden.

Dabei gilt es Anzumerken, dass es sich hierbei um tatsächlich bemerkte und auch von den Firmen angegebene Vorfälle handelt. Die reale Ziffer könnte durchaus grösser sein, da einige technische komplexere Angriffe weitaus schwieriger zu entdecken sind. Die Studie stellte auch fest, dass mit der Grösse eines Unternehmens auch deren Risiko stieg, von einer Cyberattacke betroffen zu sein. Gleichzeitig schlussfolgert die Studie auch, dass grössere Unternehmen auch weitaus mehr organisatorische Schutzmassnahmen ergreifen und ins Unternehmen einbetten. Eine Ausnahme bildet hier das Backup, das in einem Grossteil der Firmen vorgefunden wurde, unabhängig der Firmengrösse.

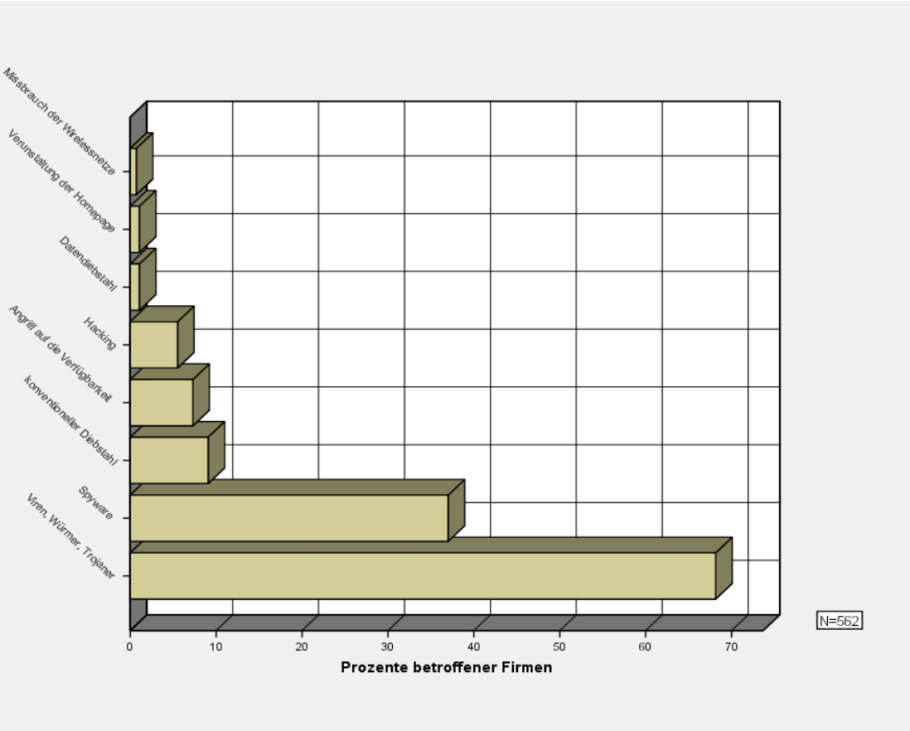

Abbildung 1.1: Häufigkeit der Vorfälle der Angriffsarten, entnommen aus der CSS-Studie [1, S. 12, Abbildung 1]

Erfreulicherweise wenden fast alle Firmen technische Sicherheitsmassnahmen an. Wie aus Abbildung 1.2 ersichtlich, erfreuen sich vor allem Antiviren und Firewalls bei fast allen Unternehmen grosser Beliebtheit.

Bei den Resultaten bezüglich der eingesetzten finanziellen Mittel zur Abwehr dieser Angriffe stellte sich heraus, dass dies besonders Branchenspezifisch zu betrachten ist. Im Unterrichtswesen sehen wir, dass mehr als die Hälfte der Unternehmen, welche zu dieser Frage Angaben machten, nicht mehr als 5000 Franken in die Informationssicherheit investiert. Im Gastgewerbe wurde ausschliesslich kleinere Beträge für die Informationssicherheit pro Firma ausgegeben.

Die Studie schlussfolgert, dass viele Unternehmen nur beschränkte finanzielle Mittel für die Gewährleistung der Informationssicherheit zur Verfügung haben. Dies zeigt sich dann auch in den personellen Anstellungen von Spezialisten, welche in der Firma für dieses Gebiet verantwortlich sind. Nur in einer Minderheit der Firmen liegt die Hauptverantwortung bei einem ausgebildeten Informatiker. In 22% der Unternehmen der Schweiz kümmert sich kein Angestellter um die Informatiksicherheit, und in 68% höchstens ein Vollzeitangestellter. Diese Vollzeitangestellten sind oftmals keine formell ausgebildeten Informatiker, sondern Personen mit nebenberuflichen Ausbil-

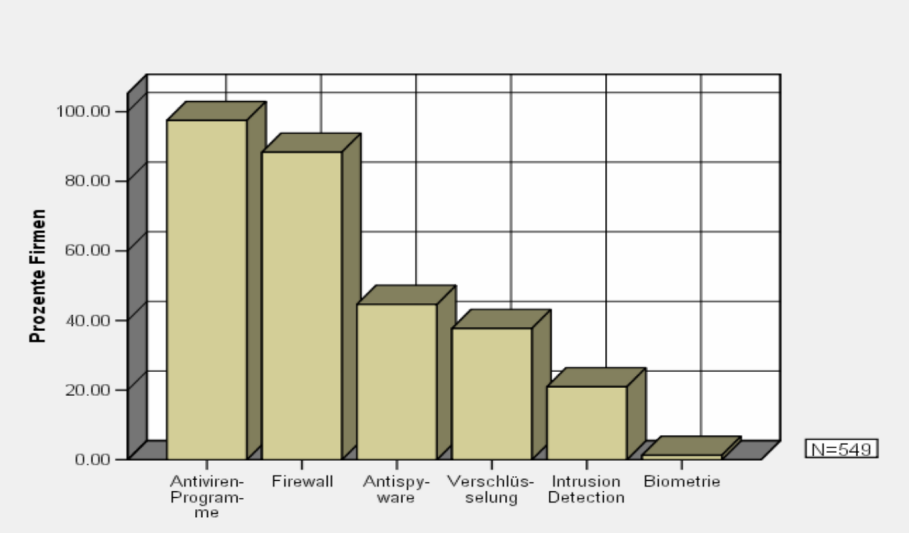

Abbildung 1.2: Häufigkeit der Anwendung von technischen Massnahmen, entnommen aus der CSS-Studie [1, S. 19, Abbildung 4]

dungen. Der Anteil von Informatikern, die in den Schweizer Unternehmen für die Informatiksicherheit verantwortlich sind, dürfte auf 15% geschätzt werden. Dies könnte auch damit zusammenhängen, dass nur 30% der befragten Firmen angaben, im Bereich der Informationssicherheit kein Outsourcing zu betreiben.

Wir sehen aus dieser Studie, dass im Jahr 2005 bereits die grosse Mehrheit der Firmen in der Schweiz einen Cyberangriff erlebten und sich mit diesem Thema auseinandersetzten. Malware machte einen Grossteil dieser Vorfälle aus. Die Mehrheit dieser Firmen setzten bereits Backups, Virenscanner und Firewalls als technische Massnahmen ein, wohingegen Intrusion Detection Systems (IDS) sehr spärlich Anwendung fanden. Je grösser eine Firma war, desto mehr Vorfälle wurden gemeldet, aber auch desto mehr organisatorische Sicherheitsmassnahmen waren vorzufinden. Allgemein holten sich viele Firmen in diesem Bereich externe Hilfe (Outsourcing), und branchenabhängig standen den Institutionen unterschiedlich grosse finanzielle Mittel für diesen Bereich zur Verfügung.

Da diese vom Bund in Auftrag gegebene Studie allerdings schon 13 Jahre her ist, möchten wir noch einen Überblick über die aktuelle Situation erhalten. Die Luzerner Hochschule hat aus eigenem Antrieb eine nationale Online-Umfrage bezüglich der Informationssicherheit in Schweizer KMU im Jahre 2016 durchgeführt, an der sich nach eigenen Angaben ca. 230 Schweizer KMU beteiligt hatten. Hier folgend einige der Punkte, die aus der Umfrage resultierte.

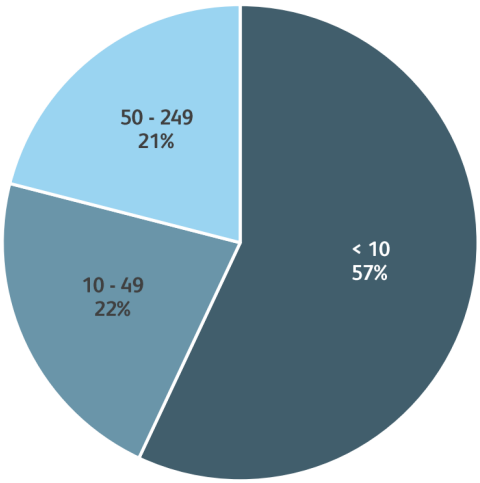

Abbildung 1.3: Verteilung der Unternehmensgrössen nach Mitarbeiteranzahl, entnommen aus der HSLU-Studie [5, S. 2, Abbildung 2]

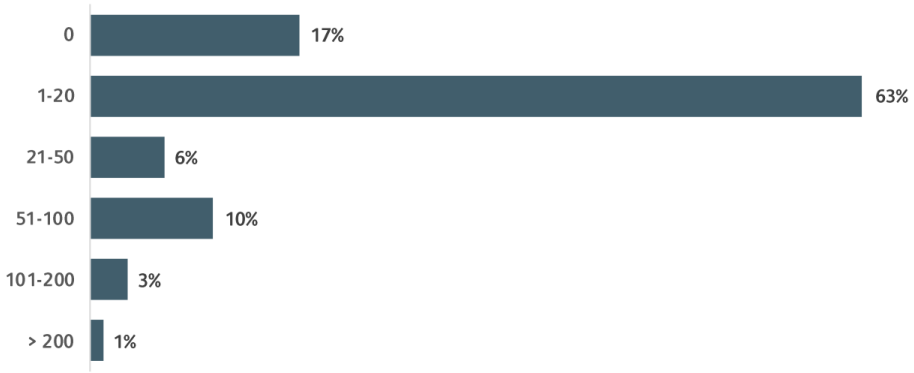

Abbildung 1.4: Verteilung der Stellenprozente für die Informationssicherheit, entnommen aus der HSLU-Studie [5, S. 7, Abbildung 12]

Die Verteilung der Unternehmensgrössen der teilnehmenden Firmen ist wichtig, da kleinere Firmen allgemein auch weniger finanzielle und personelle Ressourcen für diesen Bereich haben. Die Zusammensetzung ist in Abbildung 1.3 ersichtlich.

Rund die Hälfte aller Teilnehmenden gaben an, mindestens einen Sicherheitsvorfall in den zwölf Monaten vor der Umfrage registriert zu haben. Bei der Frage nach den Stellenprozenten für die Informationssicherheit gaben 63% an, zwischen 1-20 Stellenprozente für die Betreuung der Informationssicherheit zur Verfügung zu haben, mit 17% die gar keine Stellenprozente für dieses Gebiet haben, siehe Abbildung 1.4.

Hingegen gaben bei der Frage, ob eine Informationssicherheitspolitik ‘in

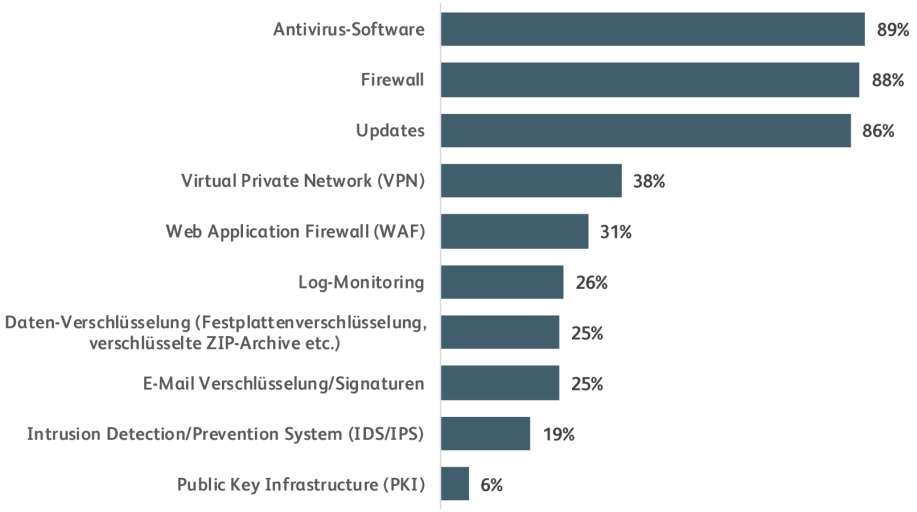

Abbildung 1.5: Verteilung der eingesetzten technischen Massnahmen, entnommen aus der HSLU-Studie [5, S. 13, Abbildung 22]

der die strategischen Informationssicherheitsziele, die Verantwortlichkeiten und Methoden für die Zielerreichung festgehalten sind' 41% an, dass bei ihnen eine solche vorhanden wäre, was relativ hoch ist in Bezug auf die Resultate der Stellenprozente. Circa ein Drittel der Befragten gab an, kein Risikomanagement anzuwenden. Bei der Frage, ob Informationssicherheitsstandards und/oder Leitfäden zur Unterstützung des Informationssicherheitsprozesses verwendet wurden, verneinte dies rund die Hälfte aller Befragten Unternehmen. Bei der Frage nach den technisch implementierten Schutzmassnahmen ergab sich Abbildung 1.5.

Auch bei der Befragung nach den Hinderungsgründen zur Umsetzung der Informationssicherheit ergab sich Abbildung 1.6.

Generell zeigt uns diese Studie, dass vielen KMU's in der Schweiz immer noch das Wissen in Bezug auf Informationssicherheit fehlt, und auch viel zu wenig Stellenprozente in dieses wichtige Gebiet investiert wird, was allerdings mit der Verteilung zu tun haben könnte, da über die Hälfte der teilnehmenden Firmen kleine Betriebe mit unter 10 Mitarbeitende hatten. Trotzdem sind die Werte viel zu niedrig, nur 4% aller teilnehmenden Firmen haben mehr als eine Vollzeitstelle in Stellenprozenten zur Verfügung, insgesamt nur 14% haben mindestens 50 Stellenprozente für dieses Gebiet, obwohl 21% der teilnehmenden Firmen eine Unternehmensgrösse von mindestens 50 Personen beinhalten. Aufgrund der anderen Zusammenstellung der teilnehmenden Firmen und der Fragenstellungen ist es schwierig, diese Studie direkt mit derjenigen von 2005 zu vergleichen. Was wir aber sehen, ist, dass die Anzahl von Unternehmen, in welcher sich gar niemand um die Informationssicherheit kümmert (was 0 Stellenprozenten entspricht) laut diesen

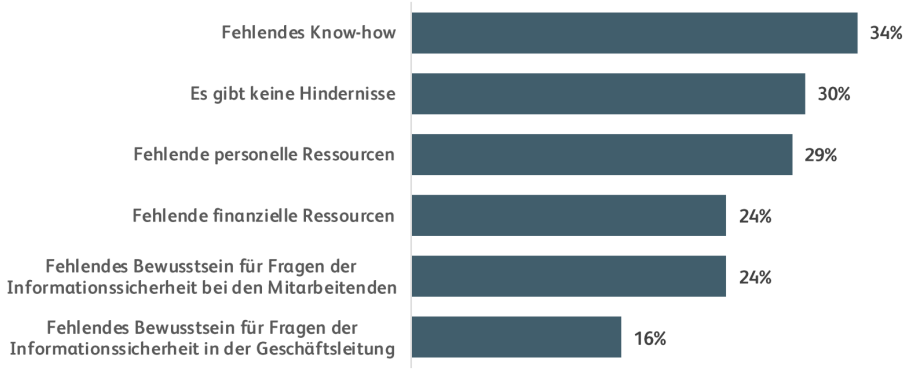

Abbildung 1.6: Verteilung der genannten Hindernisursachen bezüglich der Umsetzung von Informationssicherheit, entnommen aus der HSLU-Studie [5, S. 14, Abbildung 24]

Studien von 22% im Jahre 2005 auf 17% im Jahre 2016 verringerte. Dies ist besonders in Anbetracht dessen erfreulich, dass in der aktuelleren Studie die kleinen Unternehmen (<10 Mitarbeiter) eine grosse Gewichtung hält. Auch ist hier anzumerken, dass der hohe Anteil, in der Backups, Antivirensoftware, Firewalls und Updates angewandt wird, erfreulich ist.

Laut einer Umfrage von KMPG [6] meldeten 88%, im Jahr 2017 eine Cyberattacke erlebt zu haben, im Vergleich zu 54% im Jahre 2016. Sie beschreiben, dass auf den ersten Blick einige Resultate ein gutes Bild vermitteln: 81% der befragten Unternehmen gaben an, dass sie über die letzten zwölf Monate ein besseres Verständnis der Cyberrisiken erhielten. 52% gaben an, ein besseres Verständnis über die Motivation, Strategie und Tools der Angreifer erlangt zu haben. KPMG bemerkt allerdings, dass die teilnehmenden Schweizer Firmen ein fehlendes Verständnis über die Wichtigkeit für die Integrierung von Cybersecurity für die Wertschöpfungskette und für ihre Geschäftsziele. Es fehle ein Verständnis, welche Systeme/Daten am kostbarsten sind und zu welchem Ausmass diese Cyberbedrohungen ausgesetzt sind.

Deloitte kam in ihrem Report [3] zum Schluss, dass gut ausgearbeitete und zielgerichtete Attacken eine signifikante Bedrohung für Unternehmen in der Schweiz darstellen. Auch das binnenwirtschaftlich orientierte Unternehmen dazu tendieren, Cyberrisiken zu unterschätzen, und das dies grosse Risiken berge. Die Unternehmen müssten auch ihr Wissen in diesem Bereiche erweitern und eine strategischere Sichtweise auf die Informationssicherheit einnehmen.

Der Bundesrat hatte im Juni 2012 die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) verabschiedet, welche die Ziele anstrebte, Cyberbedrohungen frühzeitig zu erkennen, die Widerstandsfähigkeit von

kritischen Infrastrukturen zu erhöhen und Cyber-Risiken zu reduzieren. Die Strategie enthielt 16 konkrete Massnahmen, welche bis Ende 2017 vollständig Umgesetzt wurden [3]. Laut einer Wirksamkeitsüberprüfung sei es der Schweiz gelungen, durch die Umsetzung der NCS besser auf Cyber-Risiken vorbereitet zu sein, allerdings sei dieser Schutz noch ungenügend , weshalb das ISB beauftragt wurde, eine Nachfolgestrategie für 2018-2022 zu erarbeiten, welche sich auch vermehrt an kleine und mittlere Unternehmen richten sollte [4].

All dies zeigt uns die Wichtigkeit dieses Themas auch in der Schweiz. Bereits 2005 wurde ein Grossteil der Firmen durch Malware bedroht und investierte in grundlegende technische Massnahmen, und abhängig von der Grösse und Branche auch in vermehrt in organisatorische und komplexere technische Massnahmen. Heutzutage sind die Firmen in der Schweiz nicht weniger bedroht, die Komplexität von Cyberbedrohungen nimmt sogar laufend zu. allerdings stehen heute den Firmen in der Schweiz auch Kompetenzzentren wie MELANI und GovCERT und SISA zur Verfügung. Die Einführung einer Schweizerischen Cyberstrategie und Erarbeitung einer Nachfolgestrategie dessen und die parlamentarischen Vorstösse zur Schaffung eines Cyber Security Kompetenzzentrums auf Stufe Bund zeigen uns, dass auch die politische Seite sich weiterhin der Wichtigkeit dieses Themas bewusst ist und weitere Kompetenzzentren ausbauen will. Allerdings zeigen uns die Studien auf, dass viel zu wenige Stellenprozente in den Schweizer Firmen für dieses Thema aufgeboten wird, dass viele Schweizer Unternehmen laut eigenen Angaben bereit einen Sicherheitsvorfall erlebt hatten und dass das Verständnis der Wichtigkeit der Rolle von Cybersecurity noch nicht bei allen Firmen so ausgebaut sei, vor allem, wenn diese auf den Binnenmarkt fokussiert seien.

[3] https://www.efd.admin.ch/efd/de/home/themen/informatik-und-e-government/informationssicherung-in-der-elektronischen-kommunikation.html

[4] https://www.efd.admin.ch/efd/de/home/themen/informatik-und-e-government/informationssicherung-in-der-elektronischen-kommunikation/fb-schutz_vor_cyber-risiken.html

1.2 Schweizer Hochschulen

Auch für Schweizer Hochschulen besteht das Risiko von Cyberattacken. Der Nachrichtendienst des Bundes (NDB) weist auf diesen Umstand in ihrem Projekt «Prophylax» hin:

> Unternehmen und Hochschulen sind nicht mehr einzig Kleinkriminellen mit beschränkten Fähigkeiten ausgesetzt, sondern müssen auch mit Bedrohungen und Angriffen seitens organisierter und technisch bewanderter Gruppen rechnen. Die Gefährdungslage hat sich verschlimmert; die Schutzmassnahmen sind entsprechend anzupassen [9, S. 23].

Da eine Hochschule eine komplexe Organisation ist, in welchen die Institutionen zum Teil auch selbstständig in der Anwendung von Massnahmen wie das Anfertigen von Backups agieren, kann das Erarbeiten und Umsetzten einer Cyber-Abwehrstrategie ein schwieriges Unterfangen darstellen.

Die private Stiftung SWITCH [5] versucht deshalb, die Schweizer Hochschulen durch die Bereitstellung von Diensten zu unterstützen. Sie stellt das Netzwerk für die Schweizer Hochschulen (SWITCHlan und SWITCHconnect), ist mit der Sicherheit dieser Netzwerke betraut und stellt auch Identifikationsdienste (SWITCHaai und SWITCH edu-ID) den Hochschulen zur Verfügung. Auch bezüglich Sicherheitsvorfällen durch böswillige Angreifer oder neugierige und unvorsichtige User hilft das Computer Emergency Response Team, SWITCH-CERT. Dieses deckt, laut eigenem Statement von SWITCH, wöchentlich bis zu mehreren hundert solcher Fälle auf und meldet sie den Ansprechpartnern in den Informatikdiensten der Hochschulen. SWITCH-CERT tauscht sich mit GovCERT.ch, dem nationalen Computer Emergency Response Team (GovCERT) der Schweiz aus, und behandelt vor allem die Vorfälle im akademischen Bereich, da sie auch auf die Daten ihrer Netzwerke zugreifen kann.

Zum Schutz ihrer Netzwerke setzt SWITCH hauptsächlich 4 Methoden ein: Netflow-Analyse, Malware-Analyse, Response Policy Zones (RPZ) und erweitertes Sicherheitsmonitoring (ESM).

Bei der Netflow-Analyse werden die Datenströme beobachtet, welche über ihr Netzwerk laufen. Sie analysieren dabei die Informationen über den Absender und den Empfänger einer Nachricht, und vergleichen diese mit einer Liste von IP-Adressen welche bekannterweise für kriminelle Zwecke gebraucht werden. Die Vorfälle werden den Hochschulen weitergeleitet. Bei SWITCH wurde im Jahre 2015 rund 120'000 Netflows pro Sekunde analysiert.

Bei der Malware-Analyse versucht SWITCH infizierte Systeme aus den Netflows heraus zu identifizieren. Bei einer Botnetz-Infektion zum Zombie-

[5] Alle hier folgenden Informationen bezüglich SWITCH wurden https://www.switch.ch entnommen

System, versucht die Malware, mit dem Command-and-Control-Server (C&C-Server) eine Verbindung zu erstellen, um später weitere Anweisungen zu empfangen oder gestohlene Daten zu übertragen. Um die IP-Adressen dieser Server zu ermitteln, analysiert SWITCH unter anderem auch SPAM E-Mails und gehackte Webseiten die spezifisch in der Schweiz auftauchen, da Botnetze zunehmend lokal betrieben werden. Sobald man die IP-Adressen kennt, erkennt man infizierte Geräte aus den Hochschulen und kann allenfalls auch die Server vom Netz nehmen.

RPZ arbeitet mit dem Domain Name System (DNS), bei welchem Listen von bösartigen Domain-Namen gehalten und der Zugriff zu diesen Verweigert oder auf eine Warnseite verwiesen wird. Dies ist besonders effektiv gegen den Kampf von Domain-Namen generierender Malware wie Conficker. Sobald der Domain Generation Algorithm (DGA) erforscht ist, können diese in die Liste aufgenommen werden.

Erweitertes Sicherheitsmonitoring agiert unter dem Aspekt, dass die Netflow-Analyse der heutigen Bedrohungslage alleine nicht ganz gerecht wird. So werden C&C immer häufiger über legitime Server weitergeleitet, und um diese zu Erkennen braucht es genauere Datenströmeanalysen. Deshalb möchte SWITCH in den Hochschulen Sensoren installieren, welche Kopien ausgewählter Daten aus dem Netzwerkverkehr an SWITCH senden, welche dort anhand eigener Indicators of Compromise (IOCs) untersucht werden. Dies ermöglicht eine tiefere Analyse, wodurch weitere infizierte Geräte gefunden werden können.

Natürlich sollten die Hochschulen auch die Schweizerischen Datenschutzgesetzte einhalten. Zudem ist eine Hochschule immer einem Kanton auch zugeordnet und sollte die dort geltenden zusätzlichen Datenschutzbestimmungen auch einhalten.

Kapitel 2

Bedrohungslandschaft

2.1 Cyberbedrohungen

Um die Cyberbedrohung für eine Institution wie die Universität Zürich zu erkennen, bedarf es einer umfassenden Kenntnis aller möglichen Bedrohungsarten. Allerdings sind die möglichen Angriffe und die dazu benutzten Techniken aus dem Cyberraum sehr vielfältig. Diese Angriffe beruhen zum Teil auf Schwachstellen, welche nur in einem bestimmten Zeitfenster offen waren. Auch sind die technischen Angriffe oft auf die von den anzugreifenden Institutionen benutzten Systeme, Technologien und Applikationen zugeschnitten, womit also die Popularität oder die Benutzungsrate dieser Angriffe an die Benutzungsrate dieser Technologien, Systeme und Applikationen durch Institutionen mitschwankt. Dadurch sehen wir ein zeitlich trendartiges auf- und absteigen von bestimmten beobachteten Angriffsarten auf Institutionen. Im Rahmen dieser Arbeit ist es daher sinnvoll, sich auf einige wenige Attacken zu fokussieren, welche auch als momentan wahrscheinliche Bedrohung für diese Institution wahrgenommen werden kann. Dazu können wir Hauptsächlich auf sogenannte Bedrohungslandschaftsberichte (Threat Landscape Reports) zurückgreifen. Die European Union Agency for Network and Information Security (ENISA) veröffentlicht einen solchen jährlichen Report, in der sie die Top 15 Bedrohungen aus einem gesamten Jahr auflistet, welche in Abbildung 2.1 aus dem aktuellsten Report ersichtlich sind.

Laut ENISA basiert die Positionierung dieser Cyberbedrohungen auf der Anzahl von Vorfällen, ihrer Auswirkung und der Rolle, welche diese in den anderen Bedrohungen spielt. Da jede Position im Ranking nur einer Bedrohung zugeteilt werden kann, führt dies zu der Situation, dass obwohl eine Bedrohung zugenommen hat, sie trotzdem tiefer als im Vorjahr eingestuft wird. Unter anderem liegt das daran, dass diese Bedrohung, wie zum Beispiel Phising, häufiger in anderen Bedrohungen verwendet wurde und damit andere Bedrohungen im Ranking nach unten verdrängt. Dies erklärt auch, weshalb webbasierte Angriffe und Phising so hoch eingestuft werden, da dies

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware		→
2. Web based attacks	↑	2. Web based attacks		→
3. Web application attacks	↑	3. Web application attacks		→
4. Denial of service	↑	4. Phishing		↑
5. Botnets	↑	5. Spam		↑
6. Phishing	→	6. Denial of service		↓
7. Spam	↓	7. Ransomware		↑
8. Ransomware	→	8. Botnets		↓
9. Insider threat	→	9. Insider threat		→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss		→
11. Exploit kits	↑	11. Data breaches		↑
12. Data breaches	↑	12. Identity theft		↑
13. Identity theft	↓	13. Information leakage		↑
14. Information leakage	↑	14. Exploit kits		↓
15. Cyber espionage	↓	15. Cyber espionage		→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Abbildung 2.1: Übersicht über die Top 15 Cyberbedrohungen vom Jahre 2016 und 2017, entnommen aus dem ENISA Threat Landscape Report 2017 [4, S. 9, Abbildung 1]

beliebte Angriffsvektoren sind, um Malware zu verbreiten (zum Beispiel über bösartige Uniform Resource Locators (URL) welche zu Drive-by-Downloads führen, oder bösartige Dateianhänge). Erwähnenswert ist hier noch, da aus dieser Liste nicht ersichtlich, dass laut ENISA Ransomware-Attacken die Bedrohungslandschaft im Jahre 2017 dominierten.

Wenn wir die Liste in bisschen genauer betrachten, fällt uns allerdings auf, dass nicht alle separate Bedrohungen sind, sondern zum Teil oft eine Oberkategorie oder Spezielle Form einer anderen Bedrohung. So ist zum Beispiel Ransomware der Malware zuzuordnen. Exploit kits gehören zu den web based attacks. In gleicher Manier ist Identity Theft dem Data Breach unterzuordnen. Information leakage gehört meiner Meinung gleichermassen zu Insider Threat und Data Breach. Dieses ist übrigens keine Cyberattacke, sondern kann aus einer erfolgreichen Attacke resultieren, daher ist es für mich nicht unter Cyberbedrohung zuzuordnen. Genau so stellen auch Bot-

netze, welches durch Malware kontrollierte Geräte (Zombies) unwissentlich zu einem Netzwerk zusammenschliesst, keine Bedrohung dar. Die Bedrohung kommt entweder von Malware, welches das eigene Gerät zu einem Zombie macht, oder dann den Spam und Denial of Service Attacken, welche von diesen geführt werden können um diese Attacke zu verstärken, allerdings sind alle diese Bedrohungen bereits als eigene Kategorie aufgeführt, weshalb Botnetze hier nicht erläutert werden. Auch unterscheidet sich Cyber espionage insofern von allen anderen gelisteten Bedrohungen, dass es mehr ein Motiv ist. Sie vereint viele der genannten Bedrohungen, wird aber oft durch APTs ausgeführt, welche neben komplexer Malware auch bestimmte Methoden und Techniken beinhaltet, und wird deshalb als separate Kategorie beibehalten. Insider threat und Physical manipulation/damage/theft/loss ist keine Cyberbedrohung von ausserhalb, und deshalb nicht innerhalb des Rahmens dieser Arbeit. Da dabei viele neue Aspekte anfallen (Serverstandorte, physikalischer Zugang zu Infrastruktur, räumen, Computern, ob diese festgemacht sind, ob USB-Anschlüsse vorhanden und aktiviert sind, Social Engineering Techniken wie tailgating, shoulder surfing und dumpster diving usw), könnte dies als Teil einer separaten Arbeit behandelt werden. Folgende bereinigte Liste von Cyberbedrohungen ist also für diese Arbeit wichtig:

- Malware
- Web based attacks
- Web application attacks
- Phishing
- Spam
- Denial of Service
- Cyber espionage

Nachfolgend gehen wir in diesem Kapitel ein bisschen mehr auf die gelisteten Cyberbedrohungen ein [1]:

2.1.1 Malware

Malicious Software (Malware), im Deutschen auch Schadprogramm genannt, ist ein Oberbegriff und beschreibt verschiedene Arten von störender, unerwünschter und schädlicher Software. Zu den verschiedenen Malware-Arten gehören unter anderem Remote Access Trojan (RAT), Spyware, Computerviren, Computerwürmer, Rootkits, Ransomware, Backdoors und Browser-Hijacker [2]. Durch diese können unautorisierten Zugang und Kontrolle über

[1] Für nachfolgende Beschreibungen wurden hauptsächlich die Informationen aus dem Threat Landscape Report [4] und einem Beitrag von Rapid7 namens "Common Types of Cybersecurity Attacks", auffindbar unter https://www.rapid7.com/fundamentals/types-of-attacks/, verwendet

[2] https://www.avast.com/de-de/c-malware

ein System gewonnen werden (RAT), Informationen sammeln und übermitteln (Spyware), ein System infizieren und sich selbst reproduzieren (Computerviren) und sogar über das Netzwerk selbstständig verbreiten (Computerwürmer), Administratorrechte über ein System gehalten werden (Rootkit), den Zugang zu einem System für einen bestimmten Angreifer offenhalten (Backdoor) oder die Browsereinstellungen verändern und das Opfer auf eine andere Webseite umleiten (Browser-Hijacking). Laut ENISA ist Malware immer noch die am meisten angetroffene Cyberbedrohung, und die Software wird auch allgemein immer komplexer. So gab es zum Beispiel Veröffentlichungen von Exploits (zum Beispiel 'EternalBlue') und Tools, die angeblich von der NSA stammten, die dann unter anderem in der Ransomware (später auch als Wipeware klassifiziert) WannaCry oder NotPetya verwendet wurden [3]. Auch wurde in der WannaCry Software eingebaute Wurmfähigkeiten beobachtet [4]. Symantec registrierte auch, dass auch bestimmte Techniken wie «Living off the land», in der bereits auf dem angegriffenen System laufende Programme benutzt werden, an Beliebtheit zunehmen [14]. Durch diese und andere Techniken wird die Erkennung durch Sicherheitsprogramme erschwert. Die Malware wird oft vom User unbemerkt über zum Beispiel Phising-Attacken, Drive-by-Downloads oder Ausnutzung von Software-Updatemechanismen wie bei CCleaner geschehen, eingeschleust [5]. Und nicht nur Windows-Systeme sind von Malware betroffen, sondern ist auch zunehmend für Linux und MacOS Systeme zu beobachten [15]. Vor allem aber auch die kürzlich aufgedeckten Schwachstellen wie Meltdown oder Spectre verleihen diesem Thema Aktualität. Anfangs Januar war noch keine Malware oder Cyberattacke beobachtet, die diese Lücke ausnutzen würde, und viele Hersteller von Betriebssystemen und Browsern arbeiten und liefern Updates aus. Da die Lücke aber aus den Prozessorchip-Design stammt, kann diese Gefahr erst durch ein redesign richtig gebannt werden, und das wird dauern [6].

Ransomware

Ransomware (auch Verschlüsselungstrojaner) erfreute sich steigender Beliebtheit und dominierte laut ENISA auch die threat landscape im 2017. Ransomware verschlüsselt die Dateien des infizierten Rechners und fordert vom Opfer ein entsprechendes Lösegeld für die Bereitstellung der ursprünglichen Daten (Entschlüsselung). Dazu entwickelt der Angreifer eine Ransomware, und setzt einen entsprechenden C&C-Server auf und versucht danach, Systeme mit seiner Malware zu infizieren. Laut Emsisoft baut die Ransom-

[3] https://blog.rapid7.com/2017/04/18/the-shadow-brokers-leaked-exploits-faq

[4] https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r

[5] https://blog.avast.com/update-to-the-ccleaner-5.33.6162-security-incident

[6] https://blog.avast.com/meltdown-and-spectre-yes-your-device-is-likely-vulnerable

ware, wie im Falle von cryptolocker, baut nach dem infizieren eines Systems eine sichere Kommunikationsverbindung mit diesem C&C-Server auf. Diese ist verschlüsselt, so dass weder Analytiker den ausgelesenen netzwerkverkehr analysieren können und garantiert auch dem Angreifer, dass nur er mit seiner Ransomware kommunizieren kann. Die Verschlüsselung der Kommunikation läuft mittels RSA, der Angreifer verschlüsselt die Befehle mit seinem privaten Schlüssel, die Ransomware selbst hat einen öffentlichen RSA Schlüssel bereits in seinem Code. CyprtoLocker fordert dann einen zweiten öffentlichen RSA-Schlüssel für sein spezifisches Opfer an. Dann erstellt die Ransomware einen 256-bit-AES-Schlüssel, mit dem es eine symmetrische (schneller) Verschlüsselung der Daten durchführt, verschlüsselt den AES-Schlüssel mit dem zweiten erhaltenen öffentlichen RSA Schlüssel und speichert diesen zusammen mit den verschlüsselten Daten. Um diesen wieder zu entschlüsseln, wird der private key benötigt, welche auf dem Server des Angreifers gelagert sind. Die Daten selbst werden nicht mit dem RSA-Schlüssel verschlüsselt, weil dies sonst Stunden dauern würde, wobei bei Gebrauch des AES-Schlüssels das Opfersystem innerhalb kurzer Zeit gesperrt werden kann [7].

Auch sahen wir einen enormen Anstieg dieser Attacke. Lauf SonicWall GRID Threat Network, stieg die Attacke von 3.8 Millionen Fälle im Jahre 2015 auf 638 Millionen Fälle im Jahre 2016. Dies habe wahrscheinlich mit der Verfügbarkeit von Bitcoin zu tun, und dem Ansteigen von Ransomware-as-a-service (RaaS) [8]. Laut einem Beitrag von Emsisoft wird RaaS wird über Portale im Darknet angeboten und erleichtern eine Ransomware Attacke ungemein [9]. Ein Beispiel eines solchen Angebotes ist Philadelphia, die man für 389 USD kaufen kann, und mit der man unendlich viele Samples generieren kann. Somit entfällt das entwickeln einer Ransomware. Allgemein ist auch ein grosser Anstieg von RaaS Angeboten zu beobachten, und auch die Vermarktung dieser nimmt stetig zu, so wird nicht nur mehr im Darknet damit geworben, sondern auch im Surface Web, und von Philadelphia findet man Werbevideos auf Youtube. Auch Grundsätzlich machen RaaS grosse Entwicklungen gegenüber Kundenfreundlichkeit durch intuitive und moderne Gestaltung ihrer Portale und Einfachheit der Benutzung und Bedienung. Damit kann jede Person mit einer Internetverbindung eine solche Attacke ausführen. Ein bekanntes Beispiel wäre Satan, welche diesen Prozess ungemein einfach gemacht hat. Dieses verlangt keine Nutzungskosten, sondern eine Erfolgsbeteiligung von 30%. Satan vereinfacht alles insofern, dass alles auf den Servern der Anbieter läuft. Man erstellt ein Account und generiert die Samples. Mit diesem kann man dann sein Opfer infizieren. Satan hilft auch in diesem Schritt indem man einen Dropper generieren kann, und es erstellt einem auch eine HTML Seite oder ein Word Makro um diese

[7] https://blog.emsisoft.com/de/2017/06/21/ransomware-verschluesselung/

[8] https://blog.sonicwall.com/2017/02/sonicwall-threat-report-reveals-cybersecurity-arms-race/

[9] https://blog.emsisoft.com/de/2017/12/07/ransomware-as-a-service-dienstleistung/

zu verteilen. Falls das Opfer infiziert wurde, wird eine Meldung angezeigt und links, auf denen das Opfer die Zahlungsinformationen für das Lösegeld findet. Man muss hier also keinen eigenen Server aufsetzten [10]. Auch denkbar ist eine Verbreitung von erstellten RaaS Samples über ungeschützte Remotedesktopprotokolle, nach welchem man im Internet scannen kann (oder Listen online kaufen). Diese erhöhte Verfügbarkeit und Einfachheit der Durchführung einer Ransomware-Attacke erhöht das allgemeine Risiko für jede Organisation. Durch die Gewinnbeteiligungsmodelle entstehen dem Angreifer auch praktisch keine Kosten. Die erhöhte Anzahl von Attacken stellt ein Problem dar. Laut dem 2017 Global Threat Intelligende Report von NTT Security ist das Problem ist nicht ein möglicher Datenverlust und die Lösegeldforderungen seien generell tief. Die grössten Kosten für Organisationen sei die Unfähigkeit, den Kunden während dieser Attacke ihre Dienste anzubieten und die Beschämung für die Firma, wenn die Attacke allgemein publik wird.

2.1.2 Webbasierte Angriffe

ENISA definiert webbasierte Angriffe als Attacken, welche die internetfähige Systeme und Dienste sowie den Browser mit dessen Erweiterungen, Webseiten und dessen Content Management System (CMS) und die IT-Komponenten dieser Webdienste und Webapplikationen betreffen kann. So werden zum Beispiel Schwachstellen im Browser oder dessen Erweiterungen ausgenutzt, um beim Benutzer Schadcode einzuschleusen. Oft werden diese im Zusammenhang mit der Infektion von Geräten durch Malware bei Besuch einer schädlichen Webseite, wie bei 20min geschehen [11] oder zur Ausspionierung des Opfers wie im Falle von man-in-the-browser Techniken bei Bankentrojanern benutzt. Da Webseiten in unserer heutigen digitalen Welt eine wichtige Rolle spielen, werden webbasierte Angriffe wohl weiterhin ausgebaut und eingesetzt werden.

Session Hijacking und Man-in-the-Middle Attacks

Beim browsen wird zwischen dem Computer und dem Server Daten ausgetauscht. Damit der Server den Anfragenden auch beim weiteren browsen auf Unterseiten als eingeloggten Benutzer identifizieren kann, wird dieser Verbindung eine einzigartige Session ID gegeben. Der Angreifer kann nun diese Session ID durch zum Beispiel eine XSS Attacke stehlen, sich so beim Server als den vorhin erwähnten legitimen Benutzer tarnen und auf dessen Informationen und Dienste zugreifen. In einem weiteren Fall kann sich der

[10] https://nakedsecurity.sophos.com/2017/03/07/satan-ransomware-old-name-new-business-model/

[11] https://www.nzz.ch/digital/newssite-gesperrt-mittels-20minch-malware-verbreitet-ld.12263

Angreifer als Proxy-Server dazwischenschalten, womit er jegliche Kommunikation in beide Richtungen abfängt. Dazu gibt es verschiedene Angriffsarten und Techniken. So wird zum Beispiel bei einer Rouge Access Point Attacke wird der Umstand ausgenützt, dass Wireless-Karten oft versuchen, sich automatisch mit dem Access Point zu verbinden, von welchem sie das stärkste Signal empfangen. Der Angreifer kann diesen Umstand ausnützen, indem er einen eigenen Access Point aufsetzt und sich in unmittelbare physikalische Nähe begibt, damit so für seine potenziellen Opfer sein Signal am stärksten empfangen wird und sie sich mit ihm Verbinden. Nun kann der Angreifer den Netzwerkverkehr durch ein Programm wie Wireshark ausspähen, selber Pakete in den Datenstrom einspeisen, ein Session Token abfangen und SSL Stripping benutzen, um das Opfer dazu zu zwingen, http-basierte Anfragen zu schicken (anstatt https), damit sensitive Informationen in Klartext übertragen und somit vom Angreifer abgefangen und ausgelesen werden können.

Drive-by-Attacks

Bei einem Drive-by-Download kann Schadsoftware auf das Gerät der Besuchers einer Webseite geladen werden, ohne dass von diesem Benutzer irgendeine Aktion erwartet wird. Laut Sophos läuft hierbei eine Infektion in 5 Schritten ab: Schritt 1 ist der Besuch einer infizierten, aber legitimen, Webseite, welche im Schritt 2 den Besucher auf eine Seite weiterleitet, welche von den Angreiffern kontrolliert wird, und ein Exploit Kit birgt. Im Schritt 3 scannt dieses Exploit Kit den Computer nach Schwachstellen, welche es ausnutzen kann, durch zum Beispiel veraltetet Software. Nachdem es eine Schwachstelle gefunden hat, lädt es im 4ten Schritt den spezifischen Schadcode, einen sogenannten payload, auf das Gerät und installiert damit die Malware. Im 5ten Schritt wird diese Malware ausgeführt [12].

2.1.3 Angriffe auf Webapplikationen

Laut ENISA beziehen sich diese Angriffe vor allem auf den Geltungsbereich der Laufzeitumgebung einer Webanwendung und deren Programmierschnittstellen. APIs, sei aber nicht ganz überlappungsfrei mit den webbasierten angriffen. Diese Angriffe seien beliebt, da diese Dienste und Applikationen öffentlich zugänglich sind. Diese Angriffe zielen auch oft auf weit verbreitete Frameworks und Content Management Systems (CMS) ab, denn sobald eine Schwachstelle gefunden wurde, kann ein Scanner programmiert werden, welcher das Internet nach Ressourcen scannt, welche besagte verwundbare Komponente einsetzten, um anschliessend die Schwachstelle auszunutzen. Die von ENISA am meisten beobachteten Attacken in diesem Zusammenhang seien SQL Injection (SQLi), Local File Inclusion (LFI), Cross-site Scripting

[12] https://news.sophos.com/en-us/2014/03/26/how-malware-works-anatomy-of-a-drive-by-download-web-attack-infographic/

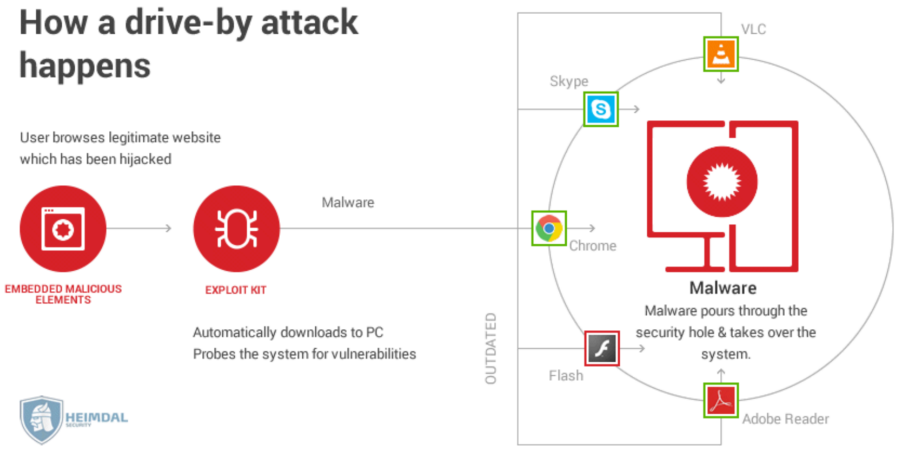

Abbildung 2.2: Ablauf einer Drive-by-Attacke, einem Beitrag von Heimdal entnommen. [13]

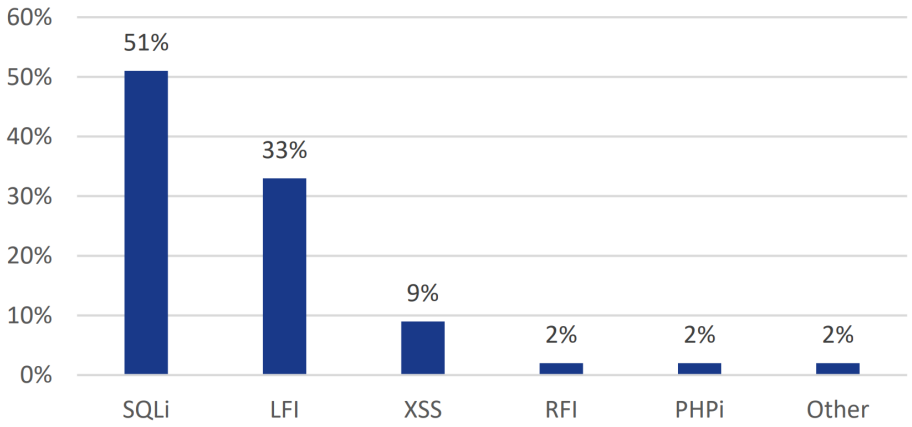

Abbildung 2.3: Übersicht über die am meisten festgestellten Attackvektoren, entnommen aus dem ENISA Threat Landscape Report 2017 [4, S. 38, Abbildung 9]

(XSS), Remote File Inclusion (RFI) und PHP Injection (PHPi), siehe dazu auch Abbildung 2.3. Auch interessant in diesem Zusammenhang ist das OWASP Top 10 Most Cirtical Application Security Risks Dokument für 2017, in der sie eine Übersicht über diese liefern, auf die einzelnen Gefahren kurz eingehen und auch mögliche anwendbare Massnahmen aufzeigen[10].

Laut Dafydd Stuttard und Marcus Pinto sind die Mehrzahl der Webapplikationen unsicher und können mit einem bescheidenen Masse an Fähigkeiten kompromittiert werden. Das Hauptproblem bestehe darin, das der

[13] https://heimdalsecurity.com/blog/how-drive-by-download-attacks-work

Anwender beliebige Eingaben an die Applikation senden könne[13, Instroduction, S. xxv]. Sie beschreiben in ihrem Buch auch unzählige Angriffsmethoden, und ein Blick in ihre Methodologie gibt einen Einblick, wie gross dieses Thema ist, und auf was alles getestet werden kann. So kann zum Beispiel die Authentifizierung, die Sitzungsverwaltung, die Zugriffskontrollen, die Datenspeicher, die Back-End Komponenten, die Applikationslogik, die Applikationsarchitektur, der Server und die Benutzer dieser Applikation selbst angegriffen werden.

Wir gehen folgend kurz auf die drei am meisten verwendete Angriffstechniken von Abbildung 2.3 ein.

Structured Query Language Injection (SQLI)

Hinter den meisten Webseiten und Diensten steht eine Datenbank, auf deren anhand Abfragen zugegriffen werden. Bei dieser Attacke versucht nun der Angreifer mit dazu ausgerichteten Abfragen die Datenbank zu einer bestimmten Aktion zu verleiten, so zum Beispiel alle gespeicherten Benutzernamen auszugeben. SQL wird dazu verwendet, Daten in einer Datenbank abzufragen, zu manipulieren und grundsächlich zu verwalten. Beim SQLI werden die Abfragen bewusst so gestaltet, um das System zu unerwarteten und vom Betreiber unerwünschten Aktionen zu veranlassen. Ein Angreifer kann so eine Authentifizierung umgehen, Daten stehlen, Daten verändern, Daten löschen und seinen eigenen Code auf der Datenbank ausführen. Dazu kann fehlende Benutzereingabeprüfung ausgenutzt werden. Des Weiteren gibt es Blind SQLI, in der der Angreifer keine direkten Daten vom Server einsieht, aber aus dem Verhalten des Systems die notwendigen Schlüsse ziehen kann, Out-of-Band Injection, in der der Angreifer die Datenbank dazu bringt, eine Verbindung mit einem eigenen, in der Kontrolle des Angreifers stehenden Systems aufzubauen. In einer Second Order Injection speichert der Angreifer eine SQL in im System zusammen mit einem Trigger, welcher zu einem bestimmten Zeitpunkt oder aufgrund einer bestimmten Aktion des Systems diese ausführt.

Local File Inclusion (LFI)

Bei der LFI wird der Umstand zunutze gemacht, dass Webseitenentwickler durch Skriptsprachen wiederverwendbarer Programmcode in unterschiedlichen Dateien speichern kann um diesen an verschiedenen Stellen als Dateien zu integrieren. Durch diese Integrationsfunktionalität dieser Programmiersprachen wird der Inhalt der Datei dann als normalen Code integriert und ausgeführt. (The Web Application Hacker's Handbook; Chapter 10 Attacking Back-End Components; File Inclusion Vulnerabilities; Page 381). Manchmal wird durch den Benutzer beeinflusst, welche Dateien genau integriert werden. Dies kann dazu führen, dass der Angreifer auf dem Server

vorhandene Funktionalitäten, auf die er sonst keinen Zugriff hätte, in einer anderen Seite einbinden und damit benützen kann[13, S. 381,382. File Inclusion Vulnerabilities].

Cross-Site Scripting (XSS)

In dieser Attacke platziert der Angreifer einen Programmcode auf einer Seite, der durch den Browser des Besuchers ausgeführt wird, sobald dieser die Webseite besucht. Generell wird zwischen reflektierte XSS, persistente XSS und DOM-basierte XSS unterschieden. Bei einer reflektierten XSS akzeptiert die Webseite Daten, die vom Webbrowser des Benutzers gesendet wird. So kann zum Beispiel ein Skript in der aufgerufenen URL selbst ausgeführt werden. In einer persistenten XSS ist das schädliche Skript, welches beim Benutzer ausgeführt wird, auf dem Server selbst gespeichert, zum Beispiel in einem Forumsbeitrag. Bei einer DOM-basierten XSS werden die benutzerseitigen Skripte, welche die Seite ausführt, so verändert, dass der Browser des Benutzers selbst wieder ein schädliches Script ausführt. In diesem Fall kann die Seite im Browser des Opfers dynamisch eine URL verändern, um schädlichen Code auszuführen.

2.1.4 Phishing

In einer Phising-Attacke versucht der Angreifer, das Opfer durch Täuschung zu einer bestimmten Aktion wie das Öffnen eines Dokumentes zu bewegen. Der Angreifer gibt vor, jemanden zu sein, dem das Opfer vertraut. Das E-Mail wird seriös gestaltet und weist meistens eine zeitliche Dringlichkeit vor mit der eine Bittet um eine bestimmte Aktion des Opfers verbunden ist. Oft findet man in diesen E-Mails ein Dokument im Anhang, welches einen bestimmten Schadcode beinhaltet, oder einen schädlichen Link im Inhalt. So könnte als Szenarien eine E-Mail vom Geschäftsführer an die Finanzabteilung eingehen, welcher sich momentan in den Ferien befindet. In dieser Mail beschreibt der Geschäftsführer, dass er eine dringende Zahlung hätte, die getätigt werden müsse, welche sich im Anhang befinde. Ein anderes Beispiel mit einem Link wäre eine Mittelung eines vom Opfer benutzten Dienstes, welches den Nutzer auf verdächtige Aktionen hinweist, die von diesem Konto aus stattgefunden haben sollten, und bittet den Nutzer, mithilfe eines Linkes, welches zum Kontrollzenter des Kontos führen sollte, dies zu kontrollieren. Beim Phising gibt es verschiedene Formen: Spear Phishing, eine speziell auf ein bestimmtes Opfer zugeschnittene Attacke. Whaling, welches wie Spear Phising ist, aber zusätzlich vor allem auf wichtige Rollen in der Firma abzielt, wie zum Beispiel dem Administrator, um bei einer erfolgreichen Attacke auch möglichst viel Zugriffsberechtigung auf das System zu haben. Beim Clone Phising wird eine bereits vom Opfer empfangene legitime Nachricht modifiziert, indem zum Beispiel ein legitimer Link mit einem

schädlichen Link (Link Spoofing) ersetzt wird. Beim Website Spoofing wird eine bereits existierende Webseite nachgebaut und vom Angreifer als echte ausgegeben, um dann die Login-Daten des ahnungslosen Opfers, welches diesen Dienst benutzen möchte, abzugreifen. Laut der infosecurity Group ist Phising ein sehr beliebter Angriffsvektor und wurde in 90-95

2.1.5 Spam

Spam ist für mehr als die Hälfte des Volumens aller E-Mails im Internet verantwortlich und wird meist durch grosse Spam-Botnetze verteilt. Oft wird durch Spammails Produkte beworben, sie können allerdings auch zur grossflächigen Malwareverteilung eingesetzt werden. Um den Erfolg solcher Mails zu steigern, werden unter anderem Informationen über das Opfer miteingebunden und Anti-Spam-Technologien eingesetzt. Grundsätzlich geht von Spam wie im Falle von Produktebewerbung keine Gefahr für Unternehmen aus. Spam kann insofern für eine Firma zu einem Problem werden, falls ein mit Malware infiziertes Gerät, welches einem Spam-Botnetz dient, aus der Firma heraus Spam verschickt. Die Firma kann so auf einer schwarzen Liste landen, welche von anderen Firmen eingesetzt werden, und so wird alle elektronische Kommunikation dieser Spam sendenden Firma von den anderen Firmen verworfen.

2.1.6 Denial of Service

Bei einer Denial of Service (DoS) Attacke, wird ein Server mit so vielen Anfragen überhäuft, dass dessen Kapazität ausgelastet ist. Dies ist vergleichbar mit dem Stau beim Gotthard. Je mehr Automobile durch den Gotthard fahren möchten, desto länger ist die Wartezeit. Dabei spielt keine Rolle, ob es sich bei dem Fahrer eines Automobils um einen Sonntagsfahrer handelt, welcher nur so zum Spass durchfährt, oder um eine Geschäftsperson handelt. So wird auch bei einer Netzwerkattacke eine massive Anzahl von Anfragen an eine Adresse gesendet, so dass auch legitime Nutzer dieses Dienstes lange Wartezeiten hinnehmen nehmen müssen, oder wie bei einer Panne in der Gotthardröhre, dieser Dienst für diese Zeit nicht mehr nutzbar ist. Laut ENISA laufen heute alle Firmen, unabhängig ihrer Grösse, Gefahr, einer DDoS-Attacke ausgesetzt zu werden. Bei dieser Attacke sehen wir auch den Trend, dass DDoS gemietet werden können. Es gibt im Internet viele Plattformen und Dienste, die sehr einfach zu bedienen sind, und eine solche Attacke jedem Individuum ermöglichen. Neben der Zugänglichkeit sind diese Attacken auch sehr günstig durchzuführen. Laut Kaspersky Lab kosten sie den Benutzer durchschnittlich 25$ pro Stunde, was circa 23.40 CHF entspricht. Die geschätzten Kosten für die Betreiber selbst belaufen sich auf 7$ pro Stunde, was rund 6.55 CHF entspricht [14]. Durch die Gewinne, die

[14] https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/

die Betreiber so einfahren, ist anzunehmen, dass die Betreiber bestimmte Kundenprogramme wie Treuerabatte aufgrund der Häufigkeit der genutzten Dienste, oder auch aufgrund der Zeitdauer der genutzten Dienste, einführen werden. ENISA weisst ausserdem darauf hin, dass DDoS-Attacken auch in Hybrid-Attacken eingesetzt werden kann, in der die lärmige und auffällige DDoS-Attacke die unauffällige Infizierung eines Systems innerhalb des Netzwerkes des Opfers überdecken sollte. ENISA listet auch die gefährlichsten DDoS-Attacken auf, unter denen sich unter anderem die Advanced Persistent DoS (APDoS), DNS Water Torture Attacks, SSL-Based Cyber Attacks und Permanent Denial of Service (PDoS) befindet. Eine APDoS verläuft über einen längeren Zeitraum und folgt einer spezifischen Motivation. DNS Water Torture Attacks betrifft die DNS Server der Angegriffenen Organisation selbst, indem sie mit schädlichen DNS-Anfragen überflutet werden. SSL-Basierte Angriffe sind den normalen ähnlich, verschlüsseln allerdings den Verkehr und fordern so durch die erforderliche Entschlüsselung einen hohen Ressourceneinsatz beim Angegriffenen System. Eine PDoS hingegen beschädigt ein System, so dass dieses ersetzt werden muss.

2.1.7 Internetspionage

Laut ENISA schaffen kriminelle Gruppen und staatlich gesponserte Gruppen neue Techniken und Tools, um intellektuelles Gut und Geheimnisse zu stehlen. Diese Techniken fallen in die Advanced Persistent Threat (APT) Kategorie. APT repräsentiere eine Kollektion von Prozessen, Tools und Ressourcen, welche benutzt werden, um ein Netzwerk zu infiltrieren und im Netzwerk über eine längere Zeit unentdeckt agieren zu können. Diese seien charakterisiert anhand der Leidenschaft und Zeit, welche in solche Attacken investiert werden. Es ist ausserdem anzunehmen, dass den Akteuren in diesem Fall grosse finanzielle Mittel zur Verfügung stehen und sie Zugriff auf Ressourcen wie Zero-Day-Exploits haben. Bei APT's können ausserdem Techniken wie «Living off the land» und datenlose Attacken eingesetzt werden, um länger unerkannt zu bleiben [14]. Der Anfang einer APT könnte das unauffällige Gegenstück bei einer bereits erwähnten Hybrid-Attacke, zusammen mit einer DDoS-Attacke, sein. Der technische Bericht von MELANI bezüglich der Untersuchung eines APT-Falles der RUAG zeigt auf, dass diese Angriffe über eine längere Zeit unerkannt bleiben können, und die Angreifer mit viel Geduld vorgehen [8]. Im Bericht wird ersichtlich, dass die Infizierung vor September 2014 stattgefunden haben muss, und erst Anfangs 2016 eine Untersuchung bezüglich dieser Attacke gestartet wurde.

2.2 Sicherheitsmassnahmen

Bei der Erarbeitung einer Abwehrstrategie gibt es verschiedene Ansätze. Wie Sacha Schweizer, Security Officer Zentrale Informatik UZH, in seiner

Lunchtalk erwähnt hatte, kann man eine Abwehr durch eine Tool-fokussierung, durch mögliche Attacktechniken, durch die Attack Chain oder durch Standards erarbeiten.

Bei der Tool-fokussierung basiert die Abwehr vor allem auf dem Einsatz bestimmter Sicherheitsprogramme. Im Internet findet man viele Artikel die mit «Die 10 besten Sicherheitsprodukte, die jedes Unternehmen einsetzten sollte». Man kümmert sich also um die Implementierung bestimmter Software, auf die man dann sein ganzes Vertrauen setzt.

Bei der Fokussierung auf Attacktechniken beschäftigt man sich mit möglichen Cyberbedrohungen, priorisiert diese, und leitet aus den möglichen Massnahmen die nächsten Schritte ab, die man bezüglich dieser Cyberbedrohung in der Firma unternehmen sollte. Bei der Attack Chain setzt man bei den einzelnen Phasen an, welche Angriffe typischerweise durchlaufen, und versucht, diesen mit geeigneten technischen und organisatorischen Massnahmen zu begegnen, um das Risiko zu vermindern.

Bei Standards werden ganze Frameworks eingesetzt, welche eine umfassendere Übersicht über die Sicherheitslage des Unternehmens durch zum Beispiel die Einführung von definierten Maturitätsleveln, was die Anwendung von Standards durch das Erfassen der gesamten Umgebung (Systeme, Netzwerke, Benutzer, Geschäftsprozesse, ...) auch viel aufwändiger macht. Bekannte Standards wären zum Beispiel das NIST Cyber Security Framework, das ISO 27001 Information Security und die SANS Ciritical Controls oder Center for Internet Security (CIS). Die National Cyber Security Alliance (NCSA), bei welcher auch Vertreter von ESET, Google Inc., Cisco und SANS mitmachen, setzt in ihrem CyberSecure My Business Programm auch auf das NIST Cybersecurity Framework.

Das NIST Framework setzt 5 Bereiche ein: Identifizieren, Schützen, Entdecken, Reagieren und Wiederherstellen. Im essentiellen Identifiziert / Bewertet man die Cybersecurity-Risiken zu seiner Organisation, danach implementiert man einen Cybersecurity-Plan, schützt seine Kunden und trainiert seine Mitarbeiter. Beim Entdecken hilft eine Awareness von Hauptbedrohungen um Sicherheitspraktiken und Verhaltensregeln einzusetzen, die diese Risiken vermindern sollten. Man setzt auch Reaktionspläne auf, die einen detaillierten Prozess aufzeigen, wie man im Falle eines Vorfalls reagieren sollte. Als letztes setzt man die Pläne auf, wie die Auswirkungen einer Attacke wieder rückgängig gemacht werden [15] [16].

Weitere Informationen und mögliche Auswirkungen zu einigen wenigen der geschilderten Cyberbedrohungen sowie mögliche Gegenmassnahmen sind im Kapitel Angriffsszenarien vorzufinden.

[15] https://staysafeonline.org/cybersecure-business/
[16] https://www.id.uzh.ch/de/dl/kurse/lunchveranstaltungen/LVP.html

Kapitel 3

Universität Zürich

3.1 Allgemein

Laut Ihrem Jahresbericht 2016 [16] wurde die Universität Zürich (UZH) in den 1830er Jahren gegründet. 1854 wurde die ETH gegründet, später wurden Mitte- und Berufsschulen neu organisiert und in den letzten Jahren gewonnen Fachhochschulen an Bedeutung, damit ist die UZH heute in ein Netz von Bildungsinstitutionen eingeflochten. Sie beschäftigt sich mit den drei Rollen als Ausbildungsstätte, Forschungseinrichtung und Arbeitgeber. Dazu strebt sie Interdisziplinarität und Interprofessionalität an, zum Beispiel durch Synergienutzung mit der ETH Zürich. Die UZH mit 25'542 Studierenden und ihren 4870 Dozierenden, darunter 661 Professorinnen und Professoren, die grösste Universität der Schweiz. Sie vergab im angegebenen Jahr 5709 Studienabschlüsse, generierte 4.9 Milliarden CHF Wertschöpfung und 41500 Arbeitsplätze. Sie besteht aus 130 Instituten und Kliniken und kooperiert mit über 1500 Institutionen in Forschung und Lehre. Sie erzielte im Jahr 2016 einen Gesamtumsatz von 1361 Mio. CHF, erhielt 293 Mio. CHF an Projektbeiträgen aus staatlichen Einrichtungen, dem Ausland, der Wirtschaft und Privaten. In den letzten 5 Jahren wurden aus der Universität 30 Spin-off-Firmen gegründet, 167 Patente eingereicht und 182 Lizenzen und Optionen vergeben. Auch in internationalen Rankings wird die Universität Zürich miteinbezogen. So wird die für das Jahr 2017 im Academic Ranking of World Universities (vormals Shanghai-Ranking) auf Platz 58, und im QA Worlds University Rankings auf Platz 80 eingeteilt, und befindet sich damit in diesen internationalen Rankings unter den Top 100 Universitäten [1]. Sie geniesst Rankings allerdings mit Vorsicht und hat sich dazu entschlossen, sich «weder organisatorisch noch strategisch an Rankings auszurichten» [2].

Die Universität organisiert sich in verschiedenen Leitungsgremien, so haben wir einen Universitätsrat, eine Universitätsleitung, eine Erweiterte

[1] http://www.uzh.ch/de/about/portrait/rankings/uzhinrankings/internationale.html
[2] http://www.uzh.ch/de/about/portrait/rankings.html

Universitätsleitung, einen Senat, die Zentralen Dienste und Unabhängige Organe [3]. Interessant für uns sind die Zentralen Dienste, worunter 'Recht und Datenschutz' und die Zentrale Informatik fallen [4]. Für den Datenschutz unterhält die Universität einen Datenschutzdeligierten, Dr. Robert Weniger. Seine Aufgabe ist es, die notwendigen Grundlagen zu erarbeiten und auch auf die Einhaltung der Datenschutzbestimmungen an der Universität durch Beratung und Kontrollen hinzuwirken [5]. Die Zentrale Informatik unterhält die IT-Infrastruktur und bietet Dienstleistungen und Anwendungen für Studenten und Institute [6]. Sie stellt damit die Grundversorgung der benötigten Informatikmittel sicher [7]. Der Zentralen Informatik ist das Strategische IT Management (SIM) unterteilt, in welchem das Information Security Management zu vorzufinden ist. Dieses erarbeitet Weisungen, überprüft deren Einhaltung, kontrolliert die laufenden Systeme auf Sicherheitslücken und betreibt operative Sicherheitssysteme, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sicherzustellen. Dafür zuständig ist der IT Security Officer der Universität Zürich, Herr Sacha Schweizer. Dies ist deshalb notwendig, da die Universität Zürich ein grosses Netzwerk betreibt, viele IT-gestützte Dienstleitungen anbietet und grosse Mengen an Daten sammelt, speichert und verarbeitet, so zum Beispiel Forschungsdaten und Ergebnisse, Adressen von immatrikulierten Studenten sowie auch Zugriffsdaten wie IP-Adressen bei Anfragen auf die UZH-Webseite [8]. Laut dem UZH Journal[12]

> nimmt auch an der Universität Zürich die Masse an Daten, die erfasst, analysiert, verarbeitet und gespeichert werden, laufend zu. Organisation und Verwaltung der UZH beruhen mittlerweile nahezu vollständig auf elektronischen Datenverarbeitungs- und Kommunikationstechniken.

Die Informatik hält eine Linux Serverfarm im Machinenraum Irchel, welcher derzeit mehr als 150 Maschinen umfasst. Dort wird die gesamte Mail-Infrastruktur, das Vorlesunsverzeichnis, die Webserver und diverse Datenbankserver unterhalten. Auf der Mehrzahl liege SuSE und SuSE Enterprise Linux. Wo sinvoll setzt die Informatik auf Open-Source Software wie Apache, Samba oder MySQL. Daneben werden komerzielle Produkte wie Oracle oder CommunigatePro eingesetzt. Die Wartung basiert auf einer SuSE AutoYaST aufbauenden Lösung [9]. Daneben betreibt die Informatik auch eine Windows-Infrastruktur [10].

[3] http://www.uzh.ch/de/about/management.html
[4] http://www.uzh.ch/de/about/management/services.html
[5] http://www.ad.uzh.ch/de/departments/legalanddataprotection/delegatefordataprotection.html
[6] http://www.id.uzh.ch/de.html
[7] http://www.id.uzh.ch/de/org/ueberuns.html
[8] https://www.uzh.ch/de/privacy
[9] https://www.uzh.ch/cmsssl/id/de/dl/bs/linux/einsatz.html
[10] https://www.uzh.ch/cmsssl/id/de/dl/bs/win-infra.html

3.2 Abwehrstrategie

Die Universität Zürich ergreift verschiedene Massnahmen, um die Universität zu schützen. Wir untersuchen dabei die uns zugänglichen Informationen, vor allem diejenigen der Webseite der zentralen Informatik. Dort hat die Universität Zürich Merkblätter und Vorschriften bezüglich der Informatiksicherheit für die Studenten, Mitarbeiter, Benutzereinheiten und IT Supervisors veröffentlicht, wo sie auf ihre Verantwortung hingewiesen werden und Sicherheitsvorschriften beim Umgang mit Informatikmitteln dargelegt werden. Neben den Merkblättern gibt es eine spezifische Unterseite, welche die Regeln für sichere Computer-Nutzung darlegt. Neben diesen Regeln gibt die zentrale Informatik auch Schutzempfehlungen aus, da sie Einzelbenutzer und Organisationseinheiten als auch verantwortlich betrachten. So empfehlen sie den Einsatz eines Antivirenprogrammes, bisher hielt die Universität eine Site-License für den McAfee-Virenscanner, welche für die Computer aller Studenten und Mitarbeiter galt. Allerdings beschränkt sich die Universität nun auf Empfehlungen von Virenschutzprogrammen. Sie weist auf weitere Massnahmen wie System-Härtung und den Einsatz einer Software-Firewall hin. Auch gibt die zentrale Informatik den Institutionen hinweise, dass diese für eine erhöhte Sicherheit ein abgesetztes Instituts-Netzwerk bilden können und durch eine eigene Hardware-Firewall ans Universitätsnetzwerk anschliessen. Dies kann untere anderem daher nötig sein, dass die zentrale Firewall der Universität nicht alle Organisationseinheiten optimal schützen kann. Da über täglich von aussen hereingetragenen Laptops, von den Antiviren noch unerkannten Malware und VPN-Verbindungen immer wieder Schadsoftware ins Universitätsnetzwerk gelangen würde [11].

Bezüglich der Verschlüsselung setzt die Universität beim Webzugriff auf eine verschlüsselte Verbindung via https mithilfe des Root-Zertifikates der UZH und bietet ausserdem verschlüsselten E-Mail-Zugriff und verschlüsselte Netzwerkzugänge durch SSH und Remote Access-VPN an. Die Universität stellt durch SWITCHpki QuoVadis Zertifikate auch Benutzerzertifikate für die Verschlüsselung oder digitale Unterzeichnung von E-Mails und PDF-Files bereit, welche Angehörige nach erfolgreicher Antragstellung beziehen können, und diese dann auch als Angehörige der UZH ausweist. Bei den technischen Massnahmen werden bei der UZH unter anderem Anti-Spam, Anti-Mailviren, Firewalls und Antispoofingtechniken eingesetzt. An den Mailgates, über welche alle E-Mails geleitet werden, werden solche, bei denen Anhänge in den EXE-, PIF-Dateien im Anhang, auch in gezippter Form, oder Mailviren entdeckt wurden, in Quarantäne gestellt. Die Universität setzt auch Antispam-Massnahmen ein, um zu verhindern, dass die Universität zu diesem Zwecke missbraucht wird und dadurch auf Anti-Spam-Listen landet. Dazu werden die Programme Spamcop und Spamman mit

[11] https://www.uzh.ch/cmsssl/id/de/dl/sicher/Empfehlungen/InstitutsFirewall.html

Spamassassing und Antispam-Listen eingesetzt sowie die Spamhaus-Listen. Zusätzlich gibt es bei den E-Mailversänden nach aussen eine Auszählung und Geo-Beurteilung, wodurch bei Unstimmigkeiten eine automatische E-Mail-Adress-Sperrung vorgenommen werden kann. Eine zentrale Firewall steht zwischen dem Universitätsnetzwerk und der Grenze zum SwitchLAN, welche Grundsätzlich alle Verbindungen gegen aussen zulässt, aber Verbindungen ins Netzwerk hinein sperrt. Diese basiert auf einer Stateful-Inspection, so dass Datenpakete, welcher keiner gültigen Session zugeordnet werden, ausgefiltert werden, so dass das Netzwerk nicht mit ungültigen Paketen erforscht werden kann. Sie hält eine Access-List (ACL) für Inbound und Outbound um IP-Adressen zu filtern, welche auf der Webseite eingesehen werden können [12]. Zusätzlich setzt die Universität dezentrale Anti-Spoofing-Filter für Subnetzwerke, und einen zentralen Anti-Spoofing-Filter ein, welche zum Beispiel alle ausgehenden Datenpakete sperrt, die als Absenderadresse eine IP-angeben, die nicht zur Universität gehört, sowie die Pakete von ausserhalb der Universitätsnetzwerkes, welche als Absenderadresse eine IP angibt, die von innerhalb des Universitätsnetzwerkes kommen müsste. Die Universität setzte auch die DNS-Firewall-Listen von Switch ein, um so auch Phishing durch die Sperrung bekannter Phisingseiten, und Botnetze durch die Sperrung bekannter DNS-Adressen der C&C-Server, entgegenzuwirken. Das Netzwerk wurde ausserdem in vier Firewall-Zonen eingeteilt in die Internet Services-Zone, die Intranet Services-Zone, die Datacenter Services-Zone und die Geschützte Zone. Für den Schutz der Endgeräte vor Viren wird ausserdem unter anderem das System Center Endpoint Protection (SCEP) Produkt von Microsoft eingesetzt.

Zur Überwachung des Netzwerks werden anfallende Netflow-Daten am Netzwerk-Eingang durch die Programme Nfsen und Argus gesammelt. Das Intrusion Detection System (IDS) Snort wurde direkt hinter der zentralen Firewall platziert, welches Vorfälle anhand von wenigen selbst erarbeiteten Regeln aus dem Entdeckungssatz 'Emerging Threats' an die IT-Security-Stelle (ITS) weiterleitet [13]. Aktiv scannende Netzwerk-Viren werden anhand eines eingesetzten No-Honey-Pot erkannt. Ein No-Honey-Pot ist eine zufällige Maschine, die Angriffe registriert, aber im Gegensatz zu einem Honey-Pot nicht speziell attraktiv oder ungeschützt für den Angreifer gemacht wurde. Zwei Sensoren verzeichnen ssh-Passwort-Attacken und der Einsatz eines zusätzlichen Botnet-Sensors wird studiert. Von dem aktiven Abscannen des Netzwerkes nach Viren wurde generell aufgrund unbefriedigender Ergebnisse abgelassen. Scanne werden allerdings mit dem Programm Arachni und OpenVAS durchgeführt, allerdings bezogen auf den Webauftritt beziehungsweise Systeminterface IP. Da das SWITCH selbst eine Netflow-Analyse und erweitertes Sicherheitsmonitoring einsetzt, bekommt auch die Universität

[12] https://www.uzh.ch/cmsssl/id/de/dl/sicher/Schutz/Transistor/TransistorDetails.html
[13] https://www.uzh.ch/cmsssl/id/de/dl/sicher/Ereignisse/Quellen.html

Zürich zum Teil standardisierte E-Mails von SWITCH-Cert betreffend anscheinend kompromittierten Systeme, welche zum Beispiel auf die Teilnahme eines bestimmten Systems aus dem Universitätsnetzwerkes an einem Botnetz aufmerksam macht [14]. Die zentrale Informatik bietet mit Globalbackup den Instituten auch einen Datensicherungsdienst an. Dazu wird der Tivoli Storage Manager (TSM) benutzt, welcher das Sichern von dezentralen Client-und Serverdaten auf einem zentralen Server ermöglicht. Die Informatikdienste sichert laut eigenen Angaben ihre Datenbestände auf diese Weise seit Mai 1995.

Auf der Datenschutzerklärung der Webseite legt die Universität unter anderem dar, dass bei jedem Aufruf/Anforderung einer UZH-Webseite bestimmte Zugriffsdaten erhoben und auf den internen Servern der UZH in einer Webserver-Logdatei abgespeichert werden. Diese können unter anderem zur Identifikation und Nachverfolgung unzulässiger Zugriffsversuche verwendet werden. Zu den erhobenen Zugriffsdaten gehören unter anderen die IP-Adresse und die Seriennummer des anfordernden Rechners, die Session-ID, Zugriffsart, Zugriffstatus und ein Zeitstempel. Diese Logs werden ab Zugriffsbeendigung für einen Zeitraum von 6 Monaten gespeichert, und danach würden sie gelöscht, ausser es sei aufgrund eines erkannten Angriffes eine weitere Speicherung dieser Daten erforderlich [15].

Die Übersicht über eine solch grosse Organisation zu halten und die Benutzerrechte sowie die damit verbundenen Datenzugriffsberechtigungen optimal zu managen, ist schwierig. Als Veranschaulichung dieses Problems möchte ich hier anführen, dass während dem Verfassen dieser Arbeit es mir möglich war, mit meinem Studentenlogin auf das inForm Datenbank Antragsformular zuzugreifen. Dort konnte ich ein neues Antragsformular bezüglich Systemberechtigung in FI/CO und HR eröffnen, und erkannte, dass es unter gewissen Punkten eine Suchmaske vorhanden war. Wenn ich eine Suche öffne und bei der Namenssuche das Prozentzeichen eingebe, gibt es mir alle SAP-BenutzerID's mit zusätzlichen Daten, was gesamthaft 5065 Einträgen entspricht, siehe Abbildung 3.1. Das Prozentzeichen wird als Wildcard-Charakter in SQL bezeichnet, und meist mit dem LIKE verwendet, welcher bei Namenssuchen oft verwendet wird, um zum Beispiel mit WHERE Name LIKE 'A%' üblicherweise alle Namen zu finden, welche mit dem Buchstaben A beginnen. Durch die alleinige Verwendung des Prozentzeichens wurden hier mit grosser Wahrscheinlichkeit alle Namen in dieser Datenbanktabelle zurückgegeben. Problematisch erscheint mir hier, dass ein normaler Bachelorstudent überhaupt Zugriff auf dieses Antragsformular, und somit die Datenbank, hat.

Als nicht ganz optimal erscheint mir auch die öffentliche Verfügbarkeit der aktuellen Service-Meldungen bezüglich IT-Security [16], siehe Abbildung

[14] https://www.uzh.ch/cmsssl/id/de/dl/sicher/Ereignisse/Quellen.html
[15] https://www.uzh.ch/de/privacy
[16] https://www.uzh.ch/id/cl/hilfe/ssl-dir/sysnews/public/index.php/newsentries?channel=

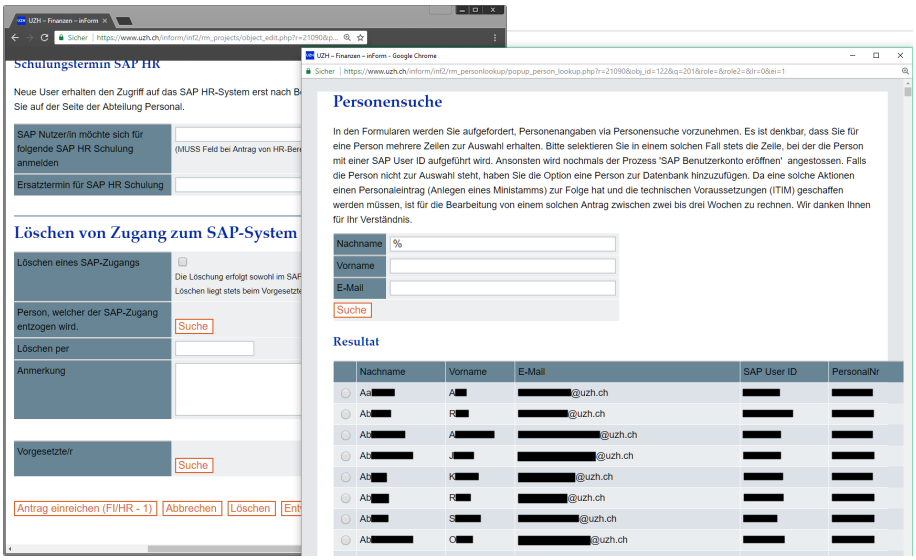

Abbildung 3.1: Screenshot der InForm-Datenbank mit dem spezifisch geschilderten Szenario. Erstellt am 30. Januar 2018 um 00:29 Uhr.

3.2 . Als Angreifer kann dies als Informationsquelle genutzt werden. Durch die Statusanzeige kann genau gesehen werden, wenn eine Sicherheitslücke noch nicht vollständig auf allen Geräten gepatcht ist, was der Angreifer zu seinem Vorteil nutzen könnte. Auch während einer Attacke kann diese Statusupdates dem Angreifer behilflich sein, da zum Beispiel die Entdeckung einer Infiltrierung oder einer getarnten Malware gepostet werden könnte. Ein Angreifer kann auch das Archiv zur Informationsbeschaffung durchforsten. So wäre zum Beispiel auffallend, dass die Universität Anfangs Januar 2018 öfters mit Switch-Problemen zu kämpfen hatte, genauer am 15.01, 12.01 16.01 und 22.01.18 wurde von Memoryproblemen von Switches, Neustarts und Stromausfällen betreffend diesen berichtet, zusätzlich zu den genauen Switch-Bezeichnungen und ihren Standorten. Dieses Archiv ist somit ein guter Startpunkt für eine OSINT in Vorbereitung einer APT, da durch all diese Informationen ein guter Einblick in das Netzwerk der UZH, Standorte und Bezeichnungen von Geräten gewonnen werden kann, und ein Angriffspunkt gewählt werden kann, indem ein oft auftretendes Problem ausgenutzt wird und so eine tatsächliche Infiltrierung getarnt werden könnte. Meiner Ansicht nach wäre es empfehlenswert, diese Information nur im Intranet und durch ein Login geschützt zur Verfügung zu stellen.

Abbildung 3.2: Screenshot der UZH-Webseite mit den aktuellen Servicemeldungen, erstellt am 31. Januar 2018 um 06:27 Uhr.

3.3 Angriffsszenarien

Folgend wird auf 3 Szenarien eingegangen, die so als Cyberattacke auf die Universität Zürich stattfinden könnte. Als Szenarien wurden eine DoS-Angriffsform, eine Ransomware-Attacke und eine APT gewählt. Diesen drei Szenarien resultieren aus den Hauptmotiven von finanziellem Gewinn und Datenbeschaffung. Die Universität Zürich hat viele finanzielle Mittel zur Verfügung. Wie bereits gezeigt, erzielte die Universität im Jahr 2016 einen Gesamtumsatz von 1361 Millionen CHF. Aus Projektbeiträgen und Drittmittel flossen der Universität im gleichen Jahr 293 Millionen CHF zu. Die Universitätsleitung verfügt auch eine Strategische Reserve, welche sich aktuell auf 13 Mio CHF beläuft [17]. Die ersten zwei Szenarien sind nun beide monetär motiviert. Sie unterscheiden sich grundlegend, da das erste Szenario eine Netzwerkattacke von aussen beschreibt und auf eine Überlastung und Unzugänglichmachung der Onlinedienste der Universität abzielt. Die Ransomware-Attacke hingegen beschreibt eine Infizierung von Systemen innerhalb des Universitätsnetzwerkes mit Malware. Da die Malware ins Netzwerk oder genauer in ein System eingeschleust werden muss, vereint diese Attacke meistens bereits eine Phising (durch Attachement oder Link) oder eine webbasierte Attacke (zum Beispiel einen Drive-by-Download).

[17] https://www.uzh.ch/cmsssl/fi/de/pl/budget/strategische-reserve.html

Die entsprechenden Gegenmassnahmen zu den in den Szenarien auch vorkommenden Bedrohungen werden daher berücksichtigt. Die beiden ersten Szenarien entsprechen sich soweit, dass beide das Opfer zur 'freiwilligen' Zahlungsüberweisung bewegen. Dies unterscheidet sie zum Beispiel von einer Banken-Trojaner-Attacke, welche auch monetär motiviert ist, allerdings mehr Phasen durchläuft. So muss zum Beispiel ein ganz bestimmtes System identifiziert und infiltriert werden, welches auch von der Universität für E-Banking benutzt wird. Danach muss als spezifisches Szenario die Malware solange in einem unentdeckten Zustand verbleiben, bis jemand die Zugangsdaten für das E-Banking eingibt (es wird in diesem Beispiel angenommen, dass keine Zweifaktorenauthentifizierung aktiviert wäre). Diese sammelt es, und versucht danach, diese Informationen unentdeckt durch das Netzwerk auszuschleusen und dem Angreifer zukommen zu lassen, welcher mit diesen Zugangsdaten aktiv auf dieses Konto zugreift, um das Geld zu entwenden. Tatsächlich spielt die Einfachheit der Durchführung einer DoS- oder Ransomware-Attacke eine grosse Rolle bei der Selektion dieser zwei als Szenarien. Wie im Kapitel 'Cyberbedrohungen' gezeigt, machen die Dienstleistungen und Plattformen, welche diese Attacken anbieten, so einfach, dass jeder Informatik-Bachelorstudent mit Leichtigkeit eine solche Attacke gegen die Universität Zürich unternehmen könnte. Da Plattformen wie Satan nur eine Gewinnbeteiligung fordern, entstehen dem Studenten durch den Angriff / die Infektionsversuche keinerlei Kosten, und solange der Student ein bisschen Denkarbeit in die Attacke steckt, ist auch das Risiko einer für den Studenten unangenehmen Konsequenz sehr unwahrscheinlich. Durch die Einfachheit dieser beiden Attacken wird das Risiko einer möglichen Anwendung gegen die Universität Zürich als hoch eingestuft. Im Distributed Denial of Service-as-a-Service (DDoSaaS) Bereich ist das Partnerprogramm mit Gewinnbeteiligung nicht anzutreffen, es wird eine zeitlich bestimmte Nutzungsgebühr erhoben. Laut Kaspersky Lab verlangen diese Dienstanbieter durchschnittlich 25$ pro Stunde [18]. An einer Universitätsveranstaltung schilderte Herr Silvio Oertli, Security Experte bei SWITCH-CERT, dass seine Niederländischen Kollegen bei SURFnet solche Attacken eher häufig registrieren. Falls man als Student für eine entsprechende Onlineprüfung noch nicht bereit sei, könne man sich eine DDoS-Attacke einkaufen, um damit eine Terminverschiebung für die Onlineprüfung zu veranlassen [19]. Falls Prüfungen an der Universität Zürich in den Cyberraum verlagert werden, wird auch dieses Szenario als Cyberbedrohung für die Universität relevant. Bei einer längeren andauernden DDoS-Attacke wie einer APDoS, wird ein einzelner Student als Akteur durch die hohen Kosten (im unten geschilderten Szenario würden durchschnittliche 10'200 Dollar resultieren) eher unwahr-

[18] https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/

[19] siehe UZH Lunchtalk Videoaufzeichnung, «Bedrohungslage Universität im Zeitalter der Digitalisierung», https://tube.switch.ch/videos/06fa302b

scheinlich. Hier wäre eine kriminelle Gruppe als Akteur anzunehmen, welche selbst ein Botnetz besitzt, und dieses auch mit Leichtigkeit einzusetzen weiss. Kaspersky Lab schätzt die Kosten einer DDoS mithilfe von 1000 Workstations auf 7 Dollar pro Stunde. Somit beliefen sich die generierten Kosten einer solchen Attacke für den geschilderten Zeitraum von 17 Tagen auf 2856 Dollar. Hier ist zu bemerken, dass dies durchschnittliche Maximalkosten sind. Falls eine Zahlung eintrifft, oder die Attacke erfolgreich, und für den Angreifer ersichtlich, mitigiert wird, obwohl der Akteur seine Attacke gegen die von ihm beobachteten Verteidigungsmassnahmen anpasst hatte, würde der Angreifer seine Attacke mit grosser Wahrscheinlichkeit beenden. APDoS wurde ausgewählt, da diese von ENISA als die Erste von den 5 gefährlichsten DDoS-Attacken aufgelistet wurde. Eine APDoS gegen die Universität verleiht einer Lösegeldforderung auch mehr Gewichtung, da einer Universität durch nur kurze Angriffe keine grossen Umsätze entgehen, wie dies bei beliebten Onlinestores bereits der Fall sein könnte. Eine APDoS ist keine theoretische, zukünftige Bedrohung, sondern wurde laut Radware, einem Cybersecurity-Dienstleister, bereits 2015 gegen ProtonMail eingesetzt [20]. Das dritte Szenario bedient sich des von ENISA aufgeführten Internetspionage-motives, und zielt auf Datenbeschaffung ab, da die UZH wertvolle Daten hält und sich an vielen Forschungsprojekten beteiligt. Aufgrund der Komplexheit einer APT, in der die Angreifer auch viel Geschick und Geduld beweisen, wird meistens von einer staatlich finanzierten Gruppe als Akteur ausgegangen. Der finanzierende Staat profitiert so von den gestohlenen Daten, welche möglicherweise auch einen Bezug zum aktuellen Wirtschaftsgeschehen und einen potenziellen Einfluss auf dieses beinhalten kann. Eine APT vereint aufgrund ihrer mehrstufigen Natur meist mehrerer Cyberbedrohungen in sich. Eine Begrenzung eines Szenarios auf nur eine einzige Cyberbedrohung war nur im Falle einer DoS-Attacke sinnvoll.

3.3.1 APDoS

Denkbares Szenario

Alle Studenten und Doktorierende, die auch im kommenden Semester Leistungen der Universität Zürich beanspruchen möchten, müssen sich online immatrikulieren. Für das Herbstsemer liegt das Zeitfenster für die Einschreibung zwischen dem 15 und 31 Mai [21]. Die Universität erhält am 14. Mai eine Drohung einer kriminellen Bande, die für diesen Zeitraum eine DoS-Attacke androht, zusammen mit einer Lösegeldforderung. Am 15. Mai wird eine DoS-Attacke ersichtlich.

Mögliche Auswirkungen

[20] https://blog.radware.com/security/2016/02/could-your-network-survive-apdos/
[21] http://www.students.uzh.ch/de/registration.html

Eine erfolgreiche DoS-Attacke könnte den Webserver betreffen, so dass die Webseite der Universität nicht mehr von aussen erreichbar ist. Somit kann den Studenten durch eine solche Attacke den Zugriff auf die Semestereinschreibung und die Modulbuchung verwehrt sein. Unter anderem wäre auch der Zugang zu den Unterrichtsmaterialen und Leistungsausweisen und Lösungsabgaben von Aufträgen bestimmter Module für die Studenten blockiert. Falls der Mailserver auch von dieser Attacke betroffen ist, wäre der E-Mailverkehr lahmgelegt.

Eine andere mögliche Auswirkung wäre ein finanzieller Schaden durch Bezahlung des Lösegeldes.

Allgemein ergreifbare Gegenmassnahmen

Vorbereitungen vor der Attacke: Idealerweise setzt sich die Institution mit der DoS-Problematik im Voraus auseinander und erstellt eine

DoS-Abwehrstrategie, bei der auch Drittparteien berücksichtigt und informiert wurden. Systeme sollten gehärtet und auf aktuellem Patch-level gehalten werden. Des Weiteren hilft eine vorgelagerte Firewall, die nur benötigte definierte Protokolle durchlässt und in derer zusätzlich viele Blockierungsregeln während eines Angriffes implementiert werden können. Potenziell gefährdete Systeme sollten an einem anderen Internet-Uplink hängen, um einfacher unter DDoS-Mitigation-Dienstleister gestellt zu werden. Ausweichmöglichkeiten implementieren, wie eine minimale, statische Webseite bei anderem Provider als die eigentliche Seite, auf die umgestellt werden kann.

Gegenmassnahmen während einer Attacke: Angriff protokollieren (Netflows, Serverlogs) und analysieren, um angemessene Gegenmassnahmen (wie Protokollfilterung und IP-Addressblockierung) einzuleiten. Es ist hier davon auszugehen, dass der Angreifer seine Strategie dieser Gegenmassnahmen laufend anpasst.

Geo-IP-Sperre kann angewendet werden, wenn sich die Benutzerschaft hauptsächlich in derselben geografischen Lage befindet. Das angegriffene System kann in Zusammenarbeit mit einem DDoS-Mitigation-Dienstleister in ein anderes Subnetz verschoben werden. Im Falle eines Angriffes sollte auch eng mit dem Internet Service Provider (ISP) zusammengearbeitet und dessen Möglichkeiten genutzt werden. Da ein DoS-Angriff im Rahmen einer Hybrid-Attacke geschehen könnte, sollte man mithilfe des Intrusion Detection Systems (IDS) die Eventualität von anderen unauffälligen Attacken und infizierungsversuchen prüfen.

Für weitere Details siehe Dokument «Massnahmen gegen DDoS Attacken» von MELANI [7].

Implementierte Schutzmassnahmen der Universität Zürich

Die Universität Zürich ist über SWITCHLan mit dem Internet verbunden. Laut dem Security Officer der UZH verlässt sich bei der Abwehr solcher

Attacken hauptsächlich auf SWITCH und deren Infrastruktur. Die Universität überarbeitet aber derzeit im Rahmen des Information Security Management System (ISMS) Projektes einen Notfallprozess, inklusive der Kommunikation. SWITCH selbst bietet laut Silvio Oertli den Hochschulen einen Dienst namens Remote Triggered Black Hole (RTBH) an, in der die Hochschulen den Verkehr einer angegriffenen IP-Adresse innerhalb ihres Zuständigkeitsbereiches auf den Border-Routern bei SWITCH Null-routen können. Dies bedeutet einfach, dass auf Seite des Internet Service Providers bereits die ganzen Datenpakete verworfen werden. Dies macht daher Sinn, dass der ISP viel höhere Bandbreiten und Kapazitäten innerhalb seines Netzwerkes besitzt, der Anschluss der Kunden allerdings viel geringere Bandbreiten aufweist. Der Nachteil dieser Methode ist, dass er Angreifer sein Ziel effektiv erreicht. Da alle Datenpakete an diese IP-Adresse verworfen werden, sind alle Dienste, die auf dieser IP-Adresse liefen, auch für legitime Benutzer nicht mehr verfügbar. Daher kann anschliessend einer alternativen Abwehrmethode gesucht werden, die legitime Nutzer durchlässt. Das RTBH Filtering ist eine sehr einfache Methode, um die Netzwerke des Angegriffenen zu entlasten. Da die Datenpakete ohne Inspektion einfach verworfen werden, werden auch keine grossen Ressourcen benötigt, wie dies bei einer Paketfilterung auf Seite des ISPs nötig wäre, wodurch der ISP durch das ressourcenintensive Filtern des Verkehrs selbst das Opfer des Angriffes werden würde [2] [22].

Durchführbarkeit einer Attacke: Einfach Auswirkung einer erfolgreichen Attacke: Mittel Geschätzte Wahrscheinlichkeit einer erfolgreich durchgeführten Attacke mit Schutzmassnahmen: Mittel Gesamthaftes Risiko dieser Bedrohung für die Universität Zürich: Mittel

3.3.2 Ransomware

Denkbares Szenario

Eine kriminelle Gruppe macht Gebrauch von Ransomware as a Service (RaaS), spezifisch kaufen sie «Philadelphia» von Rainmaker Labs. Sie setzten einen Command-and-Control Server (C&C-Server) auf, generieren Ransomwareproben, senden die Proben an ausgewählte Ziele an der Universität Zürich und verwalten die Attacke. Bei der Konfiguration im Software-Agent aktivieren sie die USB-Infektion und die Netzwerkverbreitung. Sie setzten ausserdem eine Verzögerung von 10 Tagen, nach der alle Daten auf den infizierten Geräten verschlüsselt werden und eine Meldung angezeigt wird mit einer Lösegeldforderung. Zusätzlich aktivieren sie die «russian roulette» Funktion, mit derer stündlich beliebige Daten gelöscht werden, bis der Zahlungsforderung nachgekommen wird [11].

Mögliche Auswirkungen

[22] https://tools.ietf.org/html/rfc5635

Produktivitätsverlust: Die verschlüsselten Computer sind in dieser Zeit nicht nutzbar. Bei einer solchen Verschlüsselungsaktion müssen alle befallenen Computer bereinigt / neu aufgesetzt werden und allenfalls die Backups wieder eingespielt werden.

Datenverlust: Falls von bestimmten Daten keine unverschlüsselten Backups vorhanden sind, könnten diese Daten verloren sein. Dies kann auch der Fall sein, wenn ein Backup zwar existiert, die Ransomware allerdings auch auf dieses Backup Zugriff hat, zum Beispiel durch den Speicherpfad, oder es werden automatisch synchronisierende Backuplösungen eingesetzt, welche die alten Daten immer mit der aktuellsten Version überschreibt. Dieser Datenverlust kann Angehörige der Universität Zürich betreffen (Studenten, Doktorierende, Professoren. . .) oder auch die zentrale Datenbank und zentralen Backups der Universität selbst.

Finanzieller Schaden: Bei Zahlung des Lösegeldes

Allgemein ergreifbare Gegenmassnahmen

Dem Benutzer minimale Zugriffsrechte geben um die Auswirkung einer Attacke zu minimieren.

Datensicherung welche vom System abgekapselt ist (offline). Bei einem Angriff kann man so die Systeme säubern und Daten aus der Sicherung zurückspielen. Falls keine Speicherlösung zum Zeitpunkt des Angriffes vorhanden war oder diese auch betroffen ist, die verschlüsselten Daten sichern/aufbewahren, damit sie allenfalls mit einer späteren gefundenen Lösung entschlüsselt werden können. Immer alle Sicherheitsupdates einspielen und Betriebssysteme und Programme aktuell halten. Angemessenes Verhalten (Misstrauen) bezüglich verdächtigen und unerwarteten E-Mails sowie ein sicheres Surfverhalten fördern. Auf Endgeräten aktuellen Virenschutz einsetzen und Dateiausführungen blockieren (unbekannte Dateien). Trennung von betroffenen Systemen vom Netzwerk sofern möglich. Blockierung von gefährlichen Dateianhängen (diese können auch innerhalb Archiven enthalten sein) wie .js (JavaScript), .jar (Java), .bat (Batch file), .exe (Windows executable), .cpl (Control Panel), .scr (Screensaver), .com (COM file), .pif (Program Information File), .vbs (Visual Basic Script), .ps1 (Windows PowerShell), .wsf (Windows Script File) sowie von Anhängen, welche Makros enthalten. Zu einigen Ransomwarefamilien gibt es bereits entsprechende Entschlüsselungsprogramme, welche die Daten entschlüsseln können, ohne dass ein Lösegeld bezahlt wird. Zusätzlich können auch Blocklisten verwendet werden, wie zum Beispiel dieser der abuse.ch

Implementierte Schutzmassnahmen der Universität Zürich

Datensicherung: Die Universität Zürich verwaltet eine zentrale Datensicherung und bietet auch den Instituten den Datensicherungsdienst «Globalbackup» mit dem Tivoli Storage Manager (TSM) an. Der gesamte Datenverlust würde somit auch von der Nutzungsrate dieses Dienstes von den

Instituten abhängen.

Zentrale Massnahmen gegen Mailviren: Alle E-Mails werden über die Mailgates geleitet, welche Mails mit EXE, PIF oder DLL Anhängen (auch in gezippter Form) oder bei welchen Viren erkannt wurden, in Quarantäne stellen.

Zentrale Massnahmen gegen Würmer: No-Honey-Pot & Intrusion Detection System (IDS) Snort zur Erkennung von Schadsoftware, welche das Netzwerk scannen. Die Firewall sperrt bestimmte Ports, die von diesen Netzwerk-Viren benutzt werden.

Firewall-Zonenkonzept im Datencenter Irchel: Das Datencenter Irchel ist in 5 Zonen unterteilt: Internet Services, Intranet Services, Datacenter Services, geschützte Zone. Allerdings gilt hier, dass wenn die Institute selbst Backups auf die zentralen Server einspielen können, müsste von den gleichen Rechnern her der Zugriff gegeben sein, und eine allfällige Infektion möglich.

DNS-Firewall-Listen von Switch gegen Malware und Phising. So wird versucht, die Verbindungen zu Command-and-Control-Master einzudämmen. Beim Phising verhindert es die Verbindung durch angeklickte Links zu bestimmten Addressen, für diesen Zweck bekannt sind.

Überwachung der Netflow-Daten zur Erkennung von Schadprogrammen durch Argus und Nfsen.

Durchführbarkeit einer Attacke: Mittel Auswirkung einer erfolgreichen Attacke: Hoch [23] Geschätzte Wahrscheinlichkeit einer erfolgreich durchgeführten Attacke mit Schutzmassnahmen: Mittel Gesamthaftes Risiko dieser Bedrohung für die Universität Zürich: Mittel

3.3.3 APT

Denkbares Szenario

Eine staatlich finanzierte Gruppe ausserhalb der Schweiz nahm die Universität Zürich ins Visier, zusammen mit anderen interessanten Zielen in der Schweiz (wie zum Beispiel die ETH und RUAG). Die Gruppe fokussierte sich danach auf die Informationsbeschaffung. Sie untersuchten und listeten alle Seiten und Domänen, die internen und externen IP-Adressräume der UZH [24], den IP-Netzplan für den Internetzugang der UZH [25], erstellten eine Netzwerktopologie, studierten verwundbare Ports und Dienste und die von der Universität verwendeten Sicherheitslösungen und Abwehrstrategien.

[23] Die generelle Auswirkung auf Organisationen wird als hoch erachtet, falls keine Datensicherung vorhanden ist oder diese auch von der Verschlüsselung betroffen ist (im Falle von 'Wipeware' wie WannaCry und NotPetya sind diese Daten verloren). Bei erfolgreicher Datensicherung wird die Auswirkung als «Mittel» eingestuft, da ein hoher Aufwand zu erwarten ist (Identifizierung der infizierten Geräte, der Säuberung / Neuaufsetzung dieser und dem Wiederherstellen der Daten aus der Sicherung auf die Geräte).

[24] http://www.id.uzh.ch/de/dl/dn/konfiguration/ip/ip-adressraeume.html

[25] http://www.id.uzh.ch/cl/dl/dn/doku/images_subnetze/Internet-Access.pdf

Danach erstellten Sie einen Angriffsplan. Sie schickten dann Mitte 2014 eine spezifisch für einen bestimmten Mitarbeiter gefertigte Phising-E-Mail ans Sekretariat und verleiteten diesen Mitarbeiter dazu, auf den Link zu klicken, wodurch eine Payload durch eine Browserschwachstelle auf den entsprechenden Rechner ausgeliefert wurde. Dadurch wurde das Remote Administration Tool (RAT) 'Poison Ivy' installiert. Dieses schickte ab und zu eine Befehls-Anfrage zu einem C&C Server. Von diesem infizierten Computer sammelten sie dann Anmeldedaten, und von dort aus bewegten sie sich weiter im Netzwerk fort und eskalierten Zugriffsberechtigungen bis zum Serverzugang. Sie gestalteten den C&C Datenverkehr möglichst unauffällig und tarnten ihn als normalen Webverkehr, spooften legitime Programme und Webseiten und wechselten kontinuierlich die IP-Adressen der externen C&C-Server. Durch das Portweiterleitungsprogramm 'ZXPortMap' wurde einen Tunnel aufgesetzt, und so die Firewall umgangen. Die für sie interessanten Forschungsdaten wurden gesammelt, in Archive verpackt und verschlüsselt, um den Inhalt vor möglicher Deep Packet Inspection (DPI) zu verstecken, und in kleine Stücke aufgeteilt, um diese Daten mit dem normalen Netzwerkverkehr unentdeckt herauszuschmuggeln. Alle dabei anfallenden Spuren wurden verwischt, und die Hintertür offengehalten, durch welche sie immer wieder mal wertvolle Informationen ausschleusten [26].

Mögliche Auswirkungen

Diebstahl intellektuellen Eigentums, dies könnte auch Firmen aus dem Privatwirtschaftssektor betreffen, die mit der UZH zusammenarbeiten. Identitätsdiebstahl und sammeln von Zugangsdaten. Überwachung von bestimmten Personen (zum Beispiel Professoren die in Projekten involviert sind, welche für dieses Land von Interesse sein könnte, oder Regimekritiker). Verkauf von den gesammelten Daten. Eine politisch oder wirtschaftlich motivierte Manipulation von Daten, wie zum Beispiel in Studien und Forschungsprojekten. So können Resultate im eigenen Interesse verfälscht werden oder ganze Forschungsprojekte sabotiert, und gleichzeitig im eigenen Lande zur Reife entwickelt und genutzt werden. Infiltrierung anderer Netzwerke und Institutionen, die mit der UZH verbunden sind.

Möglich wären auch Reputationsverlust / Vertrauensverlust in die UZH als einen Forschungspartner, damit auch ein Rückgang von in Auftrag gegebenen Studien aus der Privatwirtschaft. Auch eine vorübergehende Abkapslung der UZH von laufenden Projekten durch die anderen Institutionen wäre als Reaktion denkbar.

Allgemein ergreifbare Gegenmassnahmen

Diese Attacken beginnen oft mit einfacheren Tools und Techniken, bevor der Angreifer zu ausgeklügelteren Methoden greift. Aus diesem Grund sind die einfachen Schutzmechanismen, wie Antivirenprogramme, Updates

[26] http://resources.infosecinstitute.com/anatomy-of-an-apt-attack-step-by-step-approach/

und Filtersysteme für schädliche E-Mail weiterhin wichtig. Weitere mögliche Massnahmen: Integration von Data Execution Prevention (DEP) und Endpoint Threat Detection and Response (ETDR). Netzwerk segmentieren und überwachen (IDS). Kontrollen, um Missbrauch von privilegierten Benutzerkonten ausfindig zu machen. Logfiles überwachen und allenfalls analysieren mit zum Beispiel Security Information and Event Management (SIEM) Tools. Identifikation von kritischen Rollen (zum Beispiel Personen mit besonderen Zugangsberechtigungen zu Servern oder Forschungsnetzwerken). Vorschriften, Regeln und Sicherheitspraktiken implementieren. Verwundbarkeitsanalyse / Schwachstellenanalyse. Eine weisse Liste für Applikationen halten, um mitunter zu erschweren, dass Schadsoftware auf den Endsystemen installiert oder benutzt wird. Generell müssten Erkennungs- und Analysesysteme für alle Phasen eines APT Lebenszyklus vorhanden sein [17].

Implementierte Schutzmassnahmen der Universität Zürich

Siehe Schutzmassnahmen für den Ransomware-Fall, ausser der Datensicherung. Herr Schweizer sprach an seiner Lunchtalk darüber, wie mithilfe des Maturitäts-Modelles durch kombination verschiedener Standards wie beispielsweise NIST und SANS eine IT-Sicherheit gegenüber APT evaluiert und erreicht werden kann [27]. Eine konkrete Analyse sei bei der UZH derzeit im Gange.

Durchführbarkeit einer Attacke: Komplex Auswirkung einer erfolgreichen Attacke: Hoch Geschätzte Wahrscheinlichkeit einer erfolgreich durchgeführten Attacke mit Schutzmassnahmen: Hoch Gesamthaftes Risiko dieser Bedrohung für die Universität Zürich: Hoch

[27] https://www.id.uzh.ch/de/dl/kurse/lunchveranstaltungen/LVP.html

Kapitel 4

Schlussbemerkungen

Wir sehen in der generellen Lage der Schweiz, dass die Firmen zum Teil das Cyberrisiko unterschätzen, generell wenig Stellenprozente bezüglich einer solchen Funktion in den Firmen vorhanden ist, und auch fehlendes Knowhow als grösstes Hindernis im Umgang einer erfolgreichen Abwehrstrategie angegeben wurde. Technisch sind in den meisten Firmen grundlegende Massnahmen wie Firewall, Backup und Antivirenprogramme implementiert. Wir sehen bei der Entwicklung von Abwehrstrategien den Vormarsch von Standards, welche dieses Thema in den Firmen umfassender abdecken, allerdings auch aufwändiger und kostspieliger sind. Die Schweiz selbst hat die Wichtigkeit des Themas erkannt, und unternimmt wichtige Schritte zur Verbesserung der Lage, wie zum Beispiel mit der Umsetzung und Weiterentwicklung der NCS. MELANI und GovCert spielen in diesem Unterfangen eine wichtige Rolle und leisten einen wichtigen Beitrag. Für die Hochschulen steht mit SWITCH eine sehr hilfreiche Organisation zur Verfügung, welche diese durch Internetanschluss, Dienste, und Informationen unterstützt. SWITCH nimmt eine sehr aktive Rolle ein und hilft mit, infizierte Geräte in ihrem Netzwerk zu erkennen, zu lokalisieren und die entsprechende Organisation zu informieren. Wie wir beim Betrachten der Universität Zürich erkennen können, ist diese eine grosse, komplexe und vielfältig involvierte Organisation, in der ein effektiver Schutz vor Cyberrisiken sehr anspruchsvoll ist. Die Beschäftigung einer einzigen Person, dem Security Officer, welcher für die Internetsicherheit der gesamten Universität zuständig ist, erscheint mir für die Grösse und Komplexität der UZH eine sehr anspruchsvolle Stelle zu sein. Eine zusätzliche Unterstützung in diesem Bereich wäre wahrscheinlich wünschenswert. Die Cyberbedrohungslandschaft ist relativ gross, und birgt auch für die UZH ein grosses Risiko. In dieser Arbeit wurde ein Versuch unternommen, dies mit drei definierten Angriffsszenarien aufzuzeigen, welche von mir auch, aufgrund deren Verfügbarkeit und einfachen Durchführung, oder aber auch deren Rentabilität, als eher Wahrscheinlich eingeschätzt werden. Aufgrund meiner Beobachtungen empfehle ich, mit SWITCH eine individu-

elle DoS-Abwehr zu erarbeiten, welche SWITCH auch die Möglichkeit oder Vollmacht gibt, automatisch vorher definierte und vom Security Officer abgesegnete Massnahmen zu ergreifen. Silvio Oertli von SWITCH bestätigte mir, dass SWITCH auf Anfrage mit dem Security Officer gerne eine individuelle Lösung mit der jeweiligen Hochschule erarbeitet. Des Weiteren sollten auch die Benutzerzugriffsrechte im Auge behalten werden und ein eher ein minimalistischer Ansatz gewählt werden. So wäre zum Beispiel die Sperrung des Bachelorstudentenzugriffes auf die inForm-Datenbank eine gute Idee, da offenbar momentan über 25000 Studierenden SAP-Benutzerkontolöschungen beantragen, sowie diese Benutzerkonten auch aus der Datenbank auslesen können. Auch als Empfehlenswert erscheint mir die Abschirmung der Statusmeldungen bezüglich der IT-Sicherheit der Universität vor dem öffentlichen Auge, um Angreifern nicht wichtige Informationen auf dem Silbertablett zu servieren. Abschliessend sollte noch erwähnt werden, dass der Security Officer der Universität zurzeit im Rahmen des Information Security Management System Projektes die aktuelle Lage und Sicherheitsmassnahmen evaluiert und überarbeitet. Die Universität Zürich hat trotz ihrer Komplexität und wenigen Stellenprozente im Sicherheitsbereich gute und sinnvolle Sicherheitsmassnehmen implementiert und bietet den Institutionen in diesem Bereich auch wertvolle Dienste an.

Quellenverzeichnis

Literatur

[1] Center for Security Studies, ETH. *Informationssicherheit in Schweizer Unternehmen*. 2006. URL: https://www.melani.admin.ch/dam/melani/de/dokumente/informationssicherheit-studiedeutsch.pdf.download.pdf/informationssicherheit-studiedeutsch.pdf (siehe S. 3, 4).

[2] Cisco Systems. *REMOTELY TRIGGERED BLACK HOLE FILTERING— DESTINATION BASED AND SOURCE BASED*. 2005. URL: https://www.cisco.com/c/dam/en/us/products/collateral/security/ios-network-foundation-protection-nfp/prod_white_paper0900aecd80313fac.pdf (siehe S. 34).

[3] Deloitte. *Cyber Security in Switzerland*. 2014. URL: https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/audit/ch-en-audit-advisory-cyber-security-in-switzerland-08052014.pdf (siehe S. 7).

[4] European Union Agency for Network and Information Security ENISA. *ENISA Threat Landscape Report 2017*. Version 1.0. 2018. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 (siehe S. 12, 13, 18).

[5] Hochschule Luzern. *Nationale Studie zur Informationssicherheit in Schweizer KMU*. 2017. URL: https://www.hslu.ch/de-ch/informatik/forschung/themen/information-security/download-fachartikel-it-sicherheit/ (siehe S. 5–7).

[6] KPMG. *Clarity on Cyber Security*. 2017. URL: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/clarity-on-cyber-security-2017-en.pdf (siehe S. 7).

[7] MELANI / GovCERT.ch. *Massnahmen gegen DDoS Attacken*. 2015. URL: https://www.melani.admin.ch/dam/melani/de/dokumente/2015/04/Massnahmen_gegen_DDoS_Attacken.pdf.download.pdf/Massnahmen_gegen_DDoS_Attacken.pdf (siehe S. 33).

[8] MELANI:GovCERT. *APT Case RUAG:Technical Report*. 2016. URL: https://www.melani.admin.ch/dam/melani/de/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf (siehe S. 22).

[9] Nachrichtendienst des Bundes NDB. *Prophylax*. 2015. URL: https://www.vbs.admin.ch/content/vbs-internet/de/verschiedene-themen-des-vbs/die-nachrichtenbeschaffung-des-bundes/wirtschaftsspionage-in-der-schweiz.download/vbs-internet/de/publications/nachrichtendienst/Prophylax.pdf (siehe S. 9).

[10] OWASP. *OWASP Top 10 - 2017*. 2017. URL: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf (siehe S. 18).

[11] Dorka Palotay. *Ransomware as a Service (RaaS): Deconstructing Philadelphia*. 2017. URL: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/RaaS-Philadelphia.pdf (siehe S. 34).

[12] Alice Stöcklin Stefan und Werner. „Vertrauen und Datenschutz“. In: *UZH Journal* 46.2 (2016), S. 1 (siehe S. 25).

[13] Marcus Stuttard Dafydd und Pinto. *The Web Application Hacker's Hansdbook: Finding and Exploiting Security Flaws*. 2. Aufl. Wiley Publishing, Inc., 2011 (siehe S. 19, 20).

[14] Symantec. *Internet Security Threat Report - Living off the land and fileless attack techniques*. 2017. URL: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-living-off-the-land-and-fileless-attack-techniques-en.pdf (siehe S. 14, 22).

[15] AV-TEST. *Security Report 2016/17*. 2017. URL: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2016-2017.pdf (siehe S. 14).

[16] Unversität Zürich. *Jahresbericht 2016*. 2017. URL: http://www.uzh.ch/dam/public/about/portrait/annualreport/2016/order/UZH_Jahresbericht_2016.pdf (siehe S. 24).

[17] Verizon. *2016 Data Breach Investigations Report*. 2016. URL: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf (siehe S. 38).