

Swiss Vulnerability Report 2017



Pascal Mittner CEO
First Security Technology AG

Chur, 31. Mai 2017
5. Ausgabe

Swiss Vulnerability Report 2017

Inhaltsverzeichnis

1	Management Summary	4
2	Vorwort	5
3	Einführung	6
3.1	Einleitung	
3.2	Vulnerability Management (IT Schwachstellen Management)	6
3.3	Technische Details zur Prüfung	7
4	Inventarisierung	8
4.1	Hersteller von Betriebssystemen	9
4.2	Linux-Kernel-Versionen	10
4.3	Ports und Dienste	11
4.4	Web Applikationen	13
5	Schwachstellen in Verschlüsselungen	15
5.1	Poodle	15
5.2	Logjam	16
5.3	Freak	16
5.4	Drown	16
5.5	SSL/TLS-CCS Injection	17
5.6	Verschlüsselungsstärken	17
6	Falschkonfiguration als Schwachstelle	19
6.1	FTP Zugang: Zugang ohne Passwörter	19
6.2	NTLM: Informationen über das interne Netzwerk	19
6.3	SMB	21
6.4	Memcached	21
7	Fazit	22
7.1	Vulnerability Management	22
7.2	Software-Updates	23
7.3	Firewall richtig konfigurieren	23
7.4	Verschlüsselung und Passwörter	23
8	Glossary	24
8.1	CVSS	24
8.2	CVE Datenbank	24
8.3	Port (Liste mit am meisten verwendeten Diensten)	24/25
8.4	Schwachstelle	25
8.5	Vulnerability	25
8.6	Schweizer Cyberspace	25
9	Disclaimer	26

Pascal Mittner CEO
First Security Technology AG

Chur, 31. Mai 2017
5. Ausgabe

1. Management Summary

Zum fünften Mal veröffentlicht die First Security Technology AG (FST) den Swiss Vulnerability Report (SVR). Der jährliche Report dient dazu, mehr über die Sicherheit des Schweizer Cyberspace zu erfahren. Die FST ist der Schweizer Hersteller von IT-Schwachstellen-Analysesystemen. IT-Schwachstellen-Management (Vulnerability Management) ist das am stärksten aufkommende Themengebiet in der IT-Security. Die Meldungen von Schaden verursachenden Angriffen auf Firmen sowie IT-Schwachstellen nehmen dramatisch zu. Der Höhepunkt scheint dabei noch nicht erreicht zu sein. Keine Branche kann sich sicher sein und vermeintlich gut geschützte Unternehmungen trifft es genauso wie kleinere Firmen. Für einen erfolgreichen Einbruch in IT-Systeme und dem damit ermöglichten Daten- und Systemmissbrauch, nutzen Cyberkriminelle wie auch Geheimdienste, Schwachstellen aus. Schwachstellen erwartet man in der Regel bei der Software. Jedoch ermöglichen viel öfter als zunächst vermutet Falschkonfigurationen von IT-Systemen, zum Beispiel durch fehlende Identifikation oder Standard-Passwörter oder durch das unbewusste Anbieten von Diensten den Zugriff durch unberechtigte Dritte.

Die kontinuierliche Überprüfung der IT-Infrastruktur auf IT-Schwachstellen ist ein unabdingbarer Prozess geworden. Dies zeigen heute verschiedenste Anforderungen und Richtlinien. Das überarbeitete FINMA Rundschreiben 08/21 verlangt eine Inventur der IT-Infrastruktur und einen systematischen Prozess für die Identifikation und Beurteilung von IT-Risiken bei Finanzdienstleistern. Beim neuen EU-DSGVO (EU-Datenschutz-Grundverordnung) kann das Risiko hoher Strafzahlungen von bis zu 4 % des Jahresumsatzes durch ein professionelles IT-Schwachstellen-Management gemildert werden. Beim elektronischen Patientendossier (EPD) müssen die EPD-Gemeinschaften über ein funktionierendes IT-Schwachstellen-Management verfügen, um die Zertifizierung zu erlangen. Bei der nationalen Cyber-Strategie (NCS) behandelt Massnahme 3 (M3) «Verwundbarkeitsanalyse» die regelmässige Überprüfung der IKT-Infrastruktur mittels Prüfkonzept.

Kennen Sie Ihre Angriffsfläche?

Dieser Report zeigt die Angriffsfläche von Schweizer Konzernen, KMUs, Verwaltung und Privatpersonen aus Sicht des Internets. Die hier aufgezeigte Inventarisierung, durchgeführt auf über 20 Millionen IP-Adressen, gibt detaillierte Auskunft über die sichtbaren Systeme im Schweizer Internet. Die Visualisierungen verhelfen zu einer besseren Wahrnehmung der virtuellen und oftmals schwer fassbaren Risiken.

Die wesentlichsten Erkenntnisse aus der Inventarisierung sind:



- Web (448'000) und SIP (208'000 Systeme) sind die am häufigsten angebotenen Dienste
- viele Administrations-Logins für Firewalls, Router und NAS sind direkt aus dem Internet erreichbar
- sensitive Daten werden über unverschlüsselte Protokolle übermittelt
- 36'000 Datenbanken sind sichtbar
- 7'300 Drucker und Druckerdienste stehen zur Verfügung
- 3'800 Webkameras und 5'100 Streamingdienste wurden identifiziert
- Verwendung der gleichen Zertifikate auf tausenden Geräten; wer Zugriff auf den Privat-Key dafür besitzt, kann sich in eine solche Kommunikation einklinken
- 2'300 FTP-Zugänge erfordern kein Passwort; es ist davon auszugehen, dass damit geschäftskritische Daten oder schützenswerte Personendaten problemlos erreicht werden könnten
- Informationsweitergaben über Namensgebungen von IT-Systemen, welche für einen potentiellen Angriff Verwendung finden könnten

Beginnen Sie mit dem ersten Schritt: Inventarisieren Sie Ihre IT-Umgebung. Als zweiter Schritt identifizieren Sie Ihre Schwachstellen, damit Ihre IT einwandfrei läuft und keine kritischen Daten ungewollt abfliessen. Mit einer regelmässigen automatisierten Prüfung ihrer IT und einem soliden Reporting darüber können Sie die beiden Schritte effektiv und effizient durchführen und damit die Behebung der Schwachstellen ermöglichen. Die First Security Technology bietet Ihnen die richtige Lösung dazu.

2. Vorwort



Marcel Dobler

Unternehmer und Nationalrat
Mitglied der Sicherheitskommission
Präsident ICT Switzerland
Geschäftsführer dobler.swiss

Durch die veränderte Bedrohungslage und aufgrund der wachsenden Erkenntnis, dass man sich heute kaum mehr gegen Attacken schützen kann, ist ein Umdenken im Bereich der Informationssicherheit notwendig. Die Thematik hat so stark in Komplexität und Themenbreite zugenommen, dass es einem klassischen IT-Security Team kaum mehr möglich ist, ein Unternehmen adäquat gegen die IT- und Cyberbedrohungen zu schützen. Es braucht neue Sourcing-Modelle, bei denen auf ein diversifiziertes Team von Security-Spezialisten flexibel und bedarfsgerecht zugegriffen werden kann.

Um der Thematik IT-Security gerecht zu werden, konnten viele Unternehmen jahrelang auf hauseigene Spezialisten setzen. Der Verantwortungsbereich des Security Officer (CISO), der das Unternehmen zuverlässig vor schädlichen Viren und Hackern schützt, wurde oft als Nebenaufgabe vom Netzwerkteam übernommen. Heute sind viele Geschäftsprozesse so stark digitalisiert und von einer funktionierenden Informationstechnologie abhängig, dass sich die Unternehmen stärker schützen müssen. Immer mehr Kernprozesse von Unternehmen sind direkt mit leistungsfähigen IT-Lösungen verknüpft, die hohe Sicherheitsansprüche mit sich bringen – wie beispielsweise bei der Integration von Cloud Computing.

Eine wichtige Regel, die auch heute noch Gültigkeit hat, besagt, dass Komplexität Feind der Security ist. Die Komplexität der Bedrohungslage steigt jedoch enorm. Einerseits in technischer Hinsicht, durch die vielschichtig eingesetzten informationsverarbeitenden Systeme. Andererseits führt die Internationalisierung der Geschäftsprozesse zu einer komplexeren Ausgangslage – gesetzliche Auflagen und deren Implikationen auf die technische Infrastruktur steigen massiv an. Hinzu kommen moderne Arbeitsmodelle: Bring your own device, work from home, mobile computing und viele Weitere.

Cyberkriminalität findet heute nicht mehr nur in schlecht beleuchteten Kellern statt, sondern ist ein hochlukratives Geschäftsmodell, das sich zu einem Industriezweig entwickelt hat. Technische Spezialisten greifen im Auftrag andere Unternehmen an und hacken sensible Informationen. Dabei kann es sich um offengelegte Geschäftsgeheimnisse handeln oder um die Erpressung von Unternehmen durch Verschlüsselung ihrer Daten. Der Umsatz von Cyberkriminalität wird weltweit auf zwischen 300 Milliarden und eine Trillion Dollar im Jahr geschätzt.

In einer Welt, in der unsere Geschäftsprozesse direkt von einer stabil funktionierenden IT-Infrastruktur abhängen, die Komplexität dieser Infrastruktur massiv zunimmt und sich die Bedrohungslage täglich weiter zuspitzt, müssen wir uns immer mehr der Tatsache stellen, dass ein erfolgreicher Angriff nicht mehr nur eine Frage der Wahrscheinlichkeit ist. Wir müssen davon ausgehen, dass wir erfolgreich angegriffen werden, oder vielleicht schon erfolgreich angegriffen worden sind.

Um in dieser Realität bestehen zu können, brauchen Unternehmen mehr als ein klassisches IT-Security Team. Erfolgreiche Informationssicherheit benötigt heute das ausbalancierte Zusammenspiel von unterschiedlichen Spezialisten wie technische IT-Spezialisten, Prozessoptimierungs- und Rechtsspezialisten bis hin zu IT Security Architekten, Framework Spezialisten und anderen. Diese Spezialisten sind äusserst schwer zu finden und ein derart grosses Security Team im Hause zu haben ist teuer. Zudem kann das benötigte Spezialwissen je nach Projekt schnell variieren.

Vor allem in Unternehmen, welche noch keine hohe Maturität im Thema Security haben, kann Outsourcing eine interessante Alternative sein. Spezialisierte Unternehmen stellen Know-how und Erfahrung zur Verfügung und helfen eine Basis-Maturität aufzubauen. Da genau in dieser Phase sehr viele verschiedene Fähigkeiten und diversifiziertes Know-how benötigt werden, passt eine Service respektive Outsourcing-Denkweise hier besonders gut. Aber auch Unternehmen mit höherer Security-Maturität erhalten eine grössere Flexibilität, um auf Business-Anforderungen zu reagieren oder um Ressourcen-Spitzen abzudecken. Flexibilität, personelle Unabhängigkeit und Kostentransparenz in Kombination mit fachlichen Kompetenzen der Security-Spezialisten, welche ein auf die Risikobereitschaft abgestimmtes Security-Modell implementieren, führen zur Umstellung der Überzeugung, dass erfolgreiche Informationssicherheit nicht nur intern umgesetzt werden kann.

3. Einführung

3.1 Einleitung

Die automatisch generierten und detaillierten Informationen über die IT Infrastruktur, aufbereitet in einer Datenbank, bieten einen sehr hohen Nutzen. Durch die Komplexität und Veränderungen der Verantwortlichkeit (historisches Wachstum) befinden sich bei über 90 % aller Unternehmen nicht dokumentierte IT Komponenten und Dienste. Diese weisen ein sehr hohes IT Risiko auf, da sie weder gepflegt noch überwacht werden. Dies führt dazu, dass die Angriffsfläche unnötig gross ist. Durch das Bekanntwerden der Angriffsfläche ist dessen Verringerung durch den Einsatz von geringen Ressourcen möglich. Ein überschaubarer Aufwand führt so zu einem hohen Mehrwert.

Mit dem Swiss Vulnerability Report (SVR) zeigen wir die Angriffsfläche des Schweizer Cyberspace (öffentliches Internet der Schweiz/public IPs) * auf. Wir fokussieren uns auf die 56 wichtigsten Dienste* in Bezug auf Verbreitung und IT-Sicherheit. Bei der Suche nach diesen Diensten geben uns die Systeme meist zusätzliche Informationen preis: Informationen zu dem verwendeten Betriebssystem und Applikationen sowie dessen Versionen, Computernamen, Zertifikate und Verschlüsselungstechniken.

Mit dem jährlich und zum fünften Mal erscheinenden SVR zeigen wir auf, welcher aktuelle Trend im Schweizer Cyberspace herrscht und wie dieser sich verändert hat.

Für eine sichere Schweiz, für eine sichere IT.

* Definition im Glossar

Die First Security Technology AG (FST)

gehört seit Jahren zu den führenden Herstellern von IT-Schwachstellenanalyse-Software (Vulnerability Management) im deutschsprachigen Raum. Unsere Kunden aus den Branchen Energieversorgung, Gesundheitswesen, Finanzen, Industrien, Dienstleistungsbetrieben und Behörden setzen unsere Lösung für die Prüfung und Sicherstellung ihrer IT Infrastruktur ein.

3.2 Vulnerability Management (IT Schwachstellen Management)

IT-Infrastrukturen haben sicherheitsrelevante Schwachstellen. Schwachstellen entstehen durch Fehler in der Software oder Falschkonfiguration der Systeme. Sicherheitslücken können erkannt und behoben werden. Mit einer IT Schwachstellen Management Lösung (Vulnerability Management) ist dies effizient und effektiv zu erreichen.

Die Vorteile sind:



- Rechtzeitige Erkennung führt zu Risikominimierung
- Priorisierung führt zu einer erfolgreichen IT Security Strategie
- Berichte weisen die Qualität der IT aus
- Einhalten von Richtlinien und Compliance
- Erreichen von Zertifizierungen

Patch Management alleine genügt heute nicht mehr und vertrauen, dass es von alleine gut geht erst recht nicht. Nehmen Sie mit uns Kontakt auf. Gerne zeigen wir Ihnen wie Sie Ihre Herausforderungen im IT-Schwachstellen-Management meistern. Sie werden überrascht sein, wie einfach dies mit unserer Lösung möglich ist.

3.3 Technische Details zur Prüfung

Eine verteilte Scan-Node-Architektur führt eine Inventarisierung, bewusst über mehrere Tage verteilt, bei knapp 20 Millionen IP-Adressen durch. Diese IP-Adressen sind gemäss RIPE Datenbank auf Schweizer Postadressen eingetragen.

Bei einer Verbindung zu einem aktiven Port werden oftmals Informationen über die Applikation und ihre Version mitgeliefert. Zudem können Rückschlüsse auf das Betriebssystem gezogen werden. Die mitgelieferten Informationen zu einer Applikation können aber auch absichtlich verändert worden sein. Bei den Betriebssystemen lassen sich oft verschiedenste Versionen erkennen.

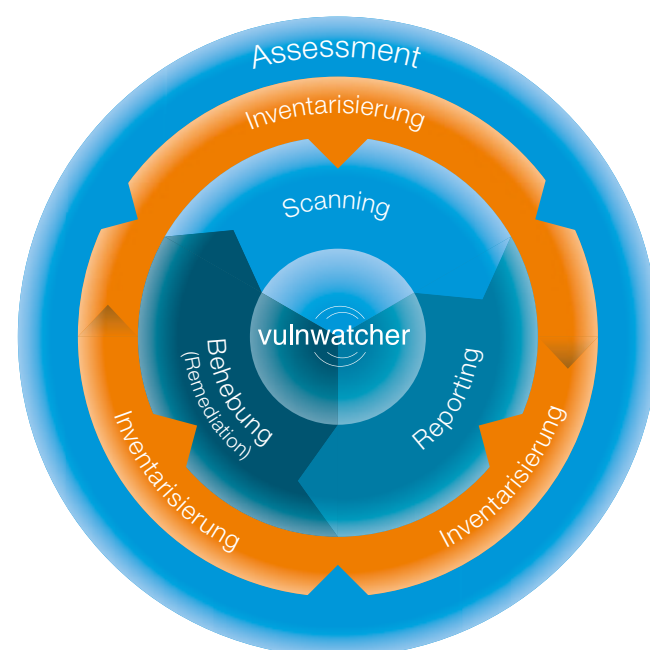
Der Bericht fasst diese Informationen zusammen und reichert diese mit interessanten Erkenntnissen an, die sich daraus gewinnen liessen.

Verfälschungen der Resultate können verschiedene Ursachen haben: Zum einen ist es einfach, die Banner der Systeme zu manipulieren und damit das tatsächliche System zu verschleiern. Dies ist eine gängige Praxis von Intrusion-Prävention-Systemen (IPS/IDS). Zudem patchen einzelne Linux-Distributoren die Applikationen in ihren Repositories oft selbst, was dazu führen kann, dass es für diese Produktversion keine Schwachstellen mehr gibt.

Rechtliches

Aus rechtlichen Gründen darf ein aktiver Security Scan, der relativ tief in ein IT-System vordringt, nicht ohne Einwilligung der Besitzer und Betreiber durchgeführt werden. Wir haben die rechtlich unproblematische Methode angewendet: Wir haben die öffentlichen Informationen zu Systemen und Versionen ausgewertet, die sich ohne Hacking-Techniken besorgen lassen.

Nur wer seine Systeme kennt, kann diese schützen.



4. Inventarisierung

19'974'213 IP-Adressen in der Schweiz
4'611'511 sichtbare Hosts
790'785 Hosts mit min. 1 aktiven Service
und insgesamt
1'396'200 aktive Services gefunden

Abbildung 1: Aktive Hosts

Bei der Prüfung von 20 Millionen IP-Adressen wurden, wie in der Einleitung beschrieben, bei über 790'000 IP-Adressen mindestens ein aktiver Dienst gefunden. Dies entspricht 4.0 % der registrierten Schweizer IP-Adressen.

Der einfachste Weg Schwachstellen zu minimieren, ist das Verringern der Angriffsfläche:

Was nicht erreichbar ist, kann nicht oder nur erschwert für Missbräuche und Attacken ausgenutzt werden. Es stellt sich bei jeder IT-Infrastruktur die Frage, welche Dienste für die eigene Geschäftstätigkeit wirklich nötig sind. Unsere Erfahrung ist, dass viele Dienste angeboten werden, derer sich die Betreiber der IT-Infrastruktur nicht bewusst sind. Diese Erkenntnis bestätigt auch der Swiss Vulnerability Report. Wir behandeln in diesem Kapitel unter anderem die identifizierten Dienste, welche idealerweise nicht direkt über das Internet ansprechbar sein sollten, da die Technologie und auch die Konfiguration nicht sicher sind.

Kennen Sie Ihre Angriffsfläche aus dem Internet? Unsere «Swiss made» Technologie hilft Ihnen, die Systeme und deren Dienste rasch zu identifizieren. Dies ist der erste Schritt um Schwachstellen zu identifizieren und zu reduzieren, bevor diese zu Ihrem Nachteil ausgenutzt werden. Sehen Sie nachfolgend einige Möglichkeiten der Inventarisierung am Beispiel der gesamten Schweizer Internet-Landschaft sowie das «Big Picture» von Diensten und deren Risiko-Potenzial, Schwachstellen auszunutzen. Es wurden Konzerne, KMUs, Kleinunternehmen und Privatpersonen in diesem Report erfasst und es sind alle von Schwachstellen betroffen, auch wenn nicht im gleichen Mass.



Abbildung 2: IP-Adressen mit aktiven Diensten in der Schweiz

Zusätzlich zur Identifikation aktiver Dienste wurde die Reaktion auf ein Ping (icmp) geprüft. 4,6 Millionen, 23 % der Schweizer IP-Adressen sprachen auf die Ping Anfrage an. Dies zeigt deutlich, dass die Mehrheit der direkt am Internet angeschlossenen Systeme auf den von

uns geprüften Ports keine Dienste anbieten. Ein solches System könnte zum Beispiel eine Firewall sein, welche nur Verkehr vom internen Netz in das Internet zulässt, aber keinen Verkehr vom Internet zu einem Dienst im internen Netzwerk weiterleitet. Internetanschlüsse von Kleinunternehmen und Privatpersonen sind meistens so konfiguriert.

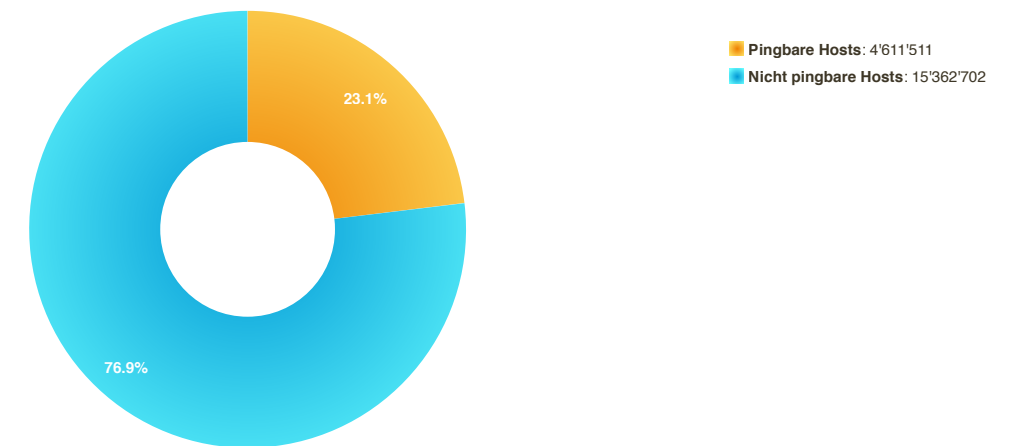


Abbildung 3: IP-Adressen in der Schweiz, welche auf ein Ping (icmp) antworten

Nur knapp 15 % der im Internet sichtbaren Systeme versuchen sich zu verstecken, indem sie nicht auf Ping reagieren.

Von den IP-Adressen mit mindestens einem aktiven Dienst sind lediglich 15 % nicht pingbar. Diese einfache Methode, um Systeme weniger sichtbar zu machen, wird offensichtlich (zu) wenig angewendet. Ein noch höheres Risiko für Angriffe gegen die eigene IT-Umgebung besteht bei pingbaren aktiven Diensten.

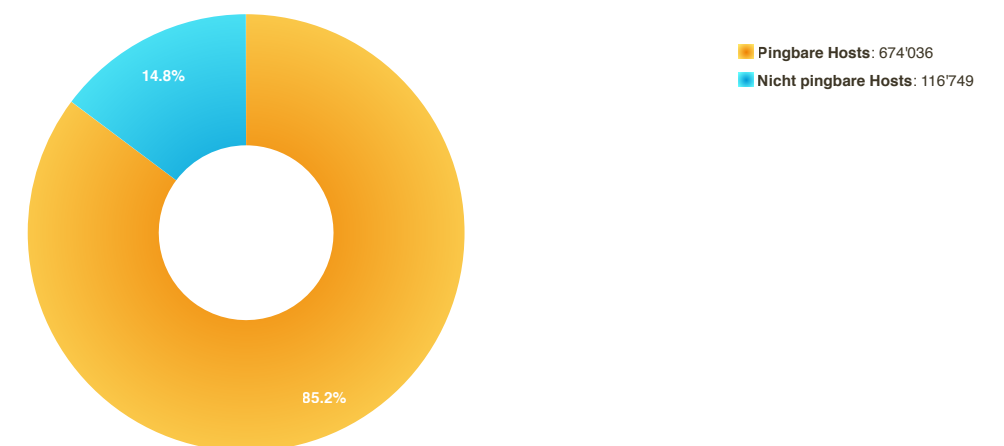


Abbildung 4: Pingbare und nicht pingbare IP-Adressen mit aktiven Diensten

4.1 Hersteller von Betriebssystemen

Seit Beginn unserer Messungen von Schwachstellen im Jahr 2013 blieb die Rangfolge der eingesetzten Betriebssysteme auf den ersten beiden Plätzen unverändert. Bei identifizierten Server-Betriebssystemen und Netzwerkkomponenten wie Firewalls und Routern, ist die Sichtbarkeit zu erwarten. Interessant ist, dass die ZyXel-Firewall an fünfter Stelle mit über 3'100 Login-Seiten für die Firewall-Administration sichtbar ist. Grundsätzlich sollte die Administrations-Seite für ein Sicherheitssystem nicht aus dem Internet erreichbar sein.

Bei 20% davon war dies sogar über einen unverschlüsselten Kanal möglich. Viele dieser Router sind wahrscheinlich mit dem Standard Passwort konfiguriert und wären damit ausgesprochen einfach manipulierbar.

eCosCentric, ein OS-Hersteller für embedded Devices, welcher verbreitet Verwendung bei der Playstation 3, Samsung Smart TVs, Parrot Sound Systems, Routern etc. findet, sticht in der Statistik ebenfalls hervor. Die meisten dieser sichtbaren Systeme sind Router. Es befinden sich auch einige Videoconferencing- und Entertainment Systeme von Technicolor darunter.

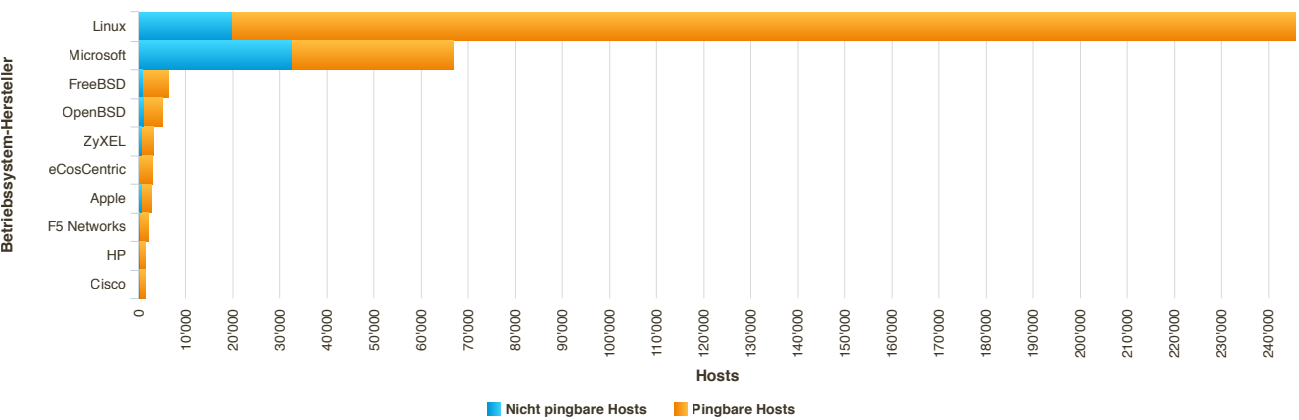


Abbildung 5: Anzahl der Betriebssysteme in der Schweiz mit Anbindung ans Internet, aufgeteilt nach Herstellern (Linux/BSD sind keine Hersteller, werden in diesem Report aber so behandelt) und die Reaktion auf ein Ping (icmp).

4.2 Linux-Kernel-Versionen

Über 245'000 Linux Betriebssysteme bieten mindestens einen Dienst an. Bei knapp 90'000 handelt es sich um http-Dienste für Administrations- und Remote-Zugriffe für Computer, Server, Firewalls, Router, Drucker, Webcams, NAS sowie klassische Webseiten. Die verschiedenen «Leaks» von Geheimdiensten zeigen einige Schwachstellen im Linux-Kernel deren verwendeter Module auf.

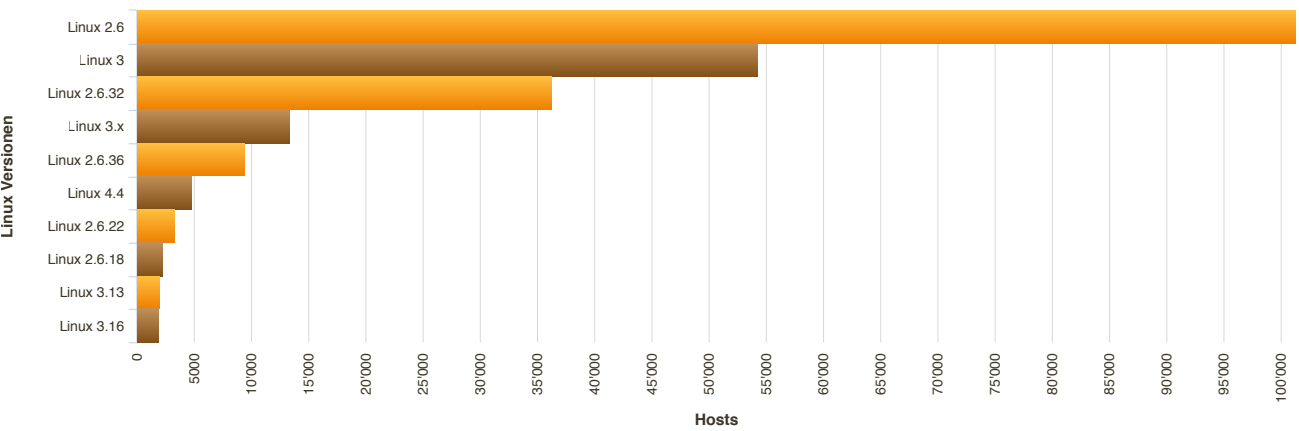


Abbildung 6: Aufteilung der Linux-Kernel-Versionen

4.3 Ports und Dienste

Die 20 Millionen IP-Adressen in der Schweiz wurden auf die 56 am häufigsten verwendeten Dienste [siehe Liste 8.3 im Anhang] überprüft. Dabei konnten knapp 1,4 Mio. aktive Dienste entdeckt werden. Fast die Hälfte dieser Dienste gaben das Produkt und die Version der Applikation preis.

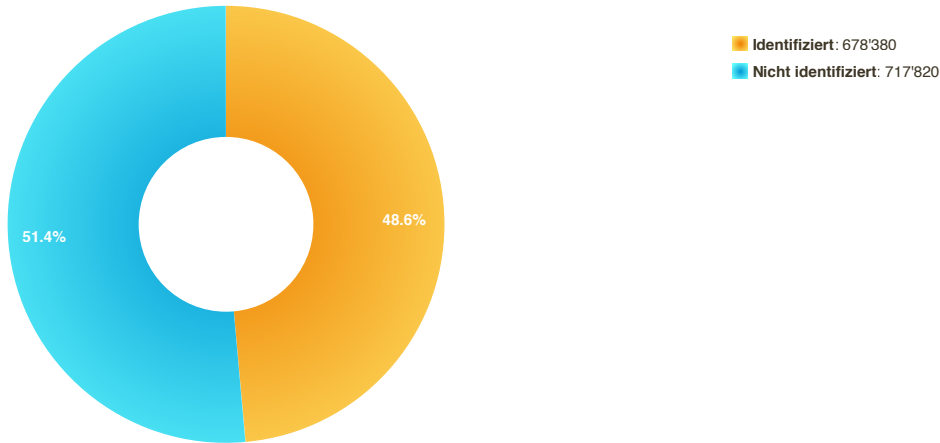


Abbildung 7: Verhältnis von identifizierten zu nicht identifizierten Produkten der aktiven Dienste

Abbildung 8 zeigt die Verteilung der aktiven Ports. Mit über 247'000 aktiven Ports ist 443/tcp führend. Die meisten dieser Ports bieten HTTPS als Service an. Seit letztem Jahr werden mehr HTTPS als die unverschlüsselte Variante HTTP verwendet. Eine positive Entwicklung hinsichtlich einer sichereren IT-Landschaft Schweiz. Offenbar fand eine Sensibilisierung statt. Allerdings ist noch unklar, wie gut die Verschlüsselungen sind. Die

Internetzugriffe sind häufig eine grosse Schwachstelle

Sind Sie sich sicher, dass Sie keinen Zugriff auf Ihre Daten über das Internet zulassen?

Durch eine regelmässige und automatisierte Überwachung Ihrer IT-Infrastruktur durch eine Vulnerability-Management-Lösung erhalten Sie diese Gewissheit und können bei einem Sicherheitsverstoß sofort reagieren.

Antworten darauf sind in Kapitel 5 ersichtlich. Das Aufkommen von Internet Telefonie über SIP veranlasste uns dieses Jahr, den Standard SIP Port 5060/tcp in die Prüfung miteinzubeziehen. Das Ergebnis überraschte uns: Mit 208'000 aktiven nimmt SIP den zweiten Platz ein. Was noch mehr erstaunt: Knapp 204'000 dieser SIP-Dienste stammen von AVM-FRITZ!Box. Bei genauerer Betrachtung der Resultate ergibt sich, dass 172'000 aus DSL-IP-Bereichen von Providern stammen. Dabei spielt ein einzelner Provider mit 169'000 SIP-aktivierten Routern die Hauptrolle. Es bleibt zu hoffen, dass die FRITZ!Box keine Schwachstellen hat, sonst kommen auf diesen Provider grosse Probleme zu. In Deutschland zeigte sich letztes Jahr, dass der Administrations-Dienst für DSL-Router zu einem Sicherheitsproblem führt. Zum Glück des Providers haben die Angreifer einen erheblichen Fehler gemacht und dadurch nur 20% der Router gehackt. Dieser Dienst ist in der Schweiz auch bei einem grossen Provider sichtbar. 135'000 der 138'000 identifizierten offenen Ports 7547/tcp stammen von ihm. Weitere Untersuchungen zeigen, dass der Zugriff auf diesen Port nur in gewissen Situationen möglich ist. Wir gehen davon aus und hoffen, dass dieser Internet-Service-Provider sich diesem Risiko bewusst ist und diesen Dienst beobachtet und daher entsprechende Sicherheitsvorkehrungen getroffen wurden.

Im Vergleich zu den Vorjahren sind unverändert über 60'000 FTP (21/tcp, unverschlüsselter Filetransfer) und 7'000 Telnet-Zugänge (23/tcp, unverschlüsselter Zugang zu einer entfernten Konsole) ersichtlich. Unverschlüsselte Protokolle sollten über das Internet nicht mehr verwendet werden, da die Möglichkeit besteht, alle Zugangsdaten mitzulesen. Die bessere Variante ist SSH (22/tcp, verschlüsselter Zugang zu einer entfernten Konsole und Filetransfer), welche über 70'000 Zugänge aufweist. Ebenfalls meist unverschlüsselt ist der HTTP Administrations-Port auf 8080/tcp. Dieser hat mit 35'000 Aktiven im Vergleich zum Vorjahr um 50% zugenommen.

Sind Ihre geschäftskritischen Daten in einer Datenbank gespeichert? Eventuell auf einer dieser 36'000 sichtbaren?

Bei Datenbanken wie MySQL (3306/tcp), MS-SQL (1433/tcp), Oracle (1521/tcp, 2484/tcp), Elasticsearch (9200/tcp), MongoDB (27017-19/tcp, 28017/19/tcp) und Hadoop (50060/tcp, 50070/tcp) sind über 36'000 aktive Systeme zu sehen. Es stellt sich die Frage, inwieweit diese aus dem Internet direkt erreichbar sein sollten, da sie meist nur durch Benutzernamen und Passwort vor Datenzugriffen geschützt sind. Wenn diese Applikationen eine Schwachstelle aufweisen, werden die Zugangsdaten für den Zugriff nicht mehr benötigt.

Sind Sie sich sicher, dass Sie keinen Zugriff auf Ihre Daten über das Internet zulassen? Durch eine regelmässige und automatisierte Überwachung Ihrer IT-Infrastruktur durch eine Vulnerability- Management-Lösung erhalten Sie diese Gewissheit und können bei einem Sicherheitsverstoß sofort reagieren.

Weitere auffällige Dienste sind Remote-Services wie VNC (5900/tcp) mit 4'500 Zugängen, welche nach unserer Erfahrung oft unverschlüsselt und ohne oder mit ungenügenden Passwörtern zum Einsatz kommen. Microsofts RDP (3389/tcp) zählt über 20'000 direkt erreichbare Administrationszugänge zu Windows Servern. Es bleibt zu hoffen, dass weder Geheimdienste, noch Cyberkriminelle unerlaubten Zugriff über Remote-Desktop haben.

9'000 SMB File Shares identifiziert

Brandaktuell ist gerade der SMB Port 445/tcp, den Wanna Cry ausnutzt, um sich zu verbreiten. Es konnten über 9'000 Systeme mit diesem offenen Port gefunden werden und 955 davon basieren auf Windows. Anscheinend sind diese alle zeitnah gepatcht worden, da es die Schweiz andernfalls viel stärker getroffen hätte. Einige Provider sperren diesen Port standardmässig, da er bereits in der Vergangenheit zu Datenübergriffen führte.

Drucken, Informationen oder Botnetz: 7'300 Drucker-Dienste stehen zur Auswahl

Drucker sind weitere Geräte mit Diensten, welche für direkten Internetzugriff Fragen aufwerfen. Diese Urgesteine der IoT (Internet of Things) wurden in der Vergangenheit mehrmals gehackt. In der Schweiz identifizierten wir 4'000 direkt ansprechbare Drucker auf dem Port 9100/tcp (raw print jobs), 2'000 IPP Dienste (631/tcp Internet Printing Protocol) für die Verwaltung von Druckaufträgen über das Netzwerk und 1'300 LPD (515/tcp Line Printer Daemon) für das Übermitteln von Druckaufträgen über das Netzwerk. Wenn diese Drucker nicht durch Authentifizierung geschützt sind, kann auf diesen über das Internet gedruckt werden. Ein Zugriff auf sensitive Informationen, im Speziellen durch das Ausnutzen von Schwachstellen, ist möglich. Über Drucker gehen im Allgemeinen doch meist sehr wichtige Informationen. Ebenfalls können diese IoT Geräte als Botnetz missbraucht werden.

Kennen Sie Ihre Angriffsfläche? Bieten Sie nur die wirklich benötigten Dienste an?

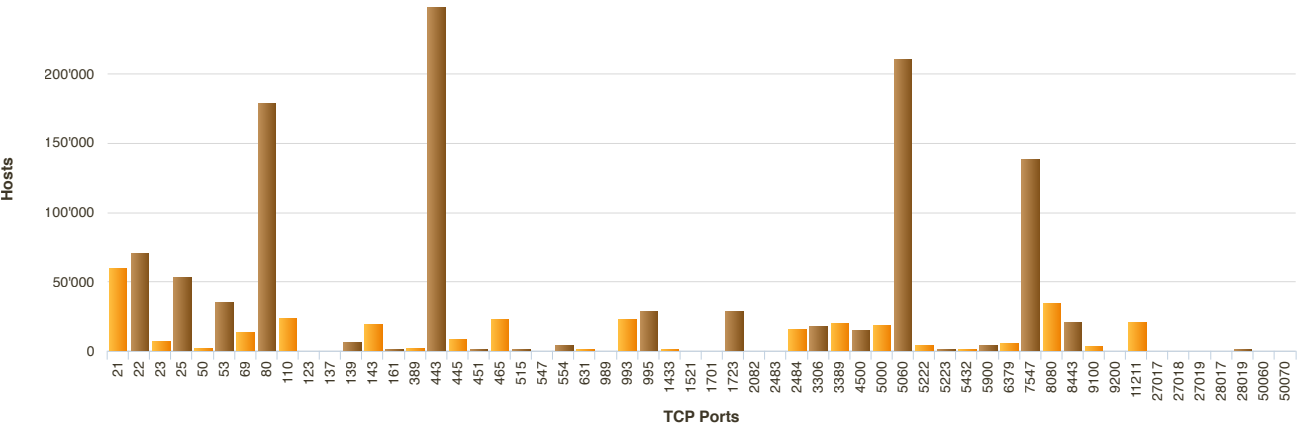


Abbildung 8: Häufigkeit der aktiven Ports

Die häufigsten Produkte benutzen die Dienste Web und E-Mail. Daneben finden sich noch SSH und FTP. Dies ist ein klarer Hinweis, für was das Internet hauptsächlich verwendet wird. Interessant ist, dass MySQL dieses Jahr die Top 10 der identifizierten Produkte erreichte.

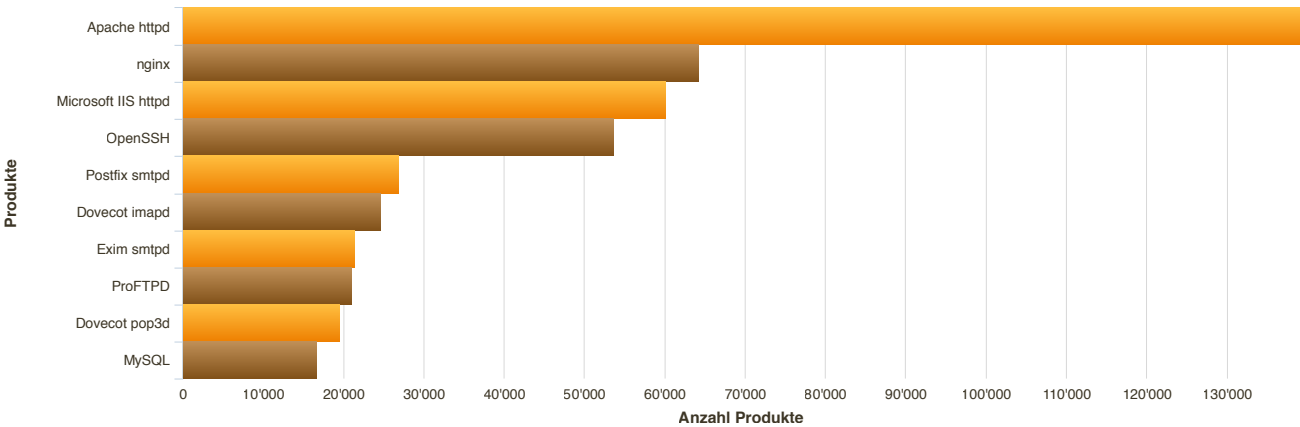


Abbildung 9: Häufigkeit der eingesetzten Produkte

Datenschutz bei Webcams

Beispielsweise betrifft die neue EU-DSGVO (EU-Datenschutz-Grundverordnung), welche ab dem 25. Mai 2018 anwendbar ist, auch Webcams in der Schweiz, wenn damit zum Beispiel ein EU-Bürger gefilmt wird. Wenn die Bussen von bis zu EUR 20 Mio. / 4 % des Jahresumsatzes auch in der Schweiz durchgesetzt werden können, wird es teuer bei Verstössen. Als Folge davon ist dann ein Businessmodell «Bussen im Datenschutz» zu befürchten. Es gilt die Praxis zu beobachten.

Wenn wir die Produkte genauer untersuchen, finden wir zum Beispiel 3'800 Webcams. Von diesen sind fast alle D-Link Webkameras. Einige Stichproben zeigen, dass die meisten passwortgeschützt sind. Dies ist sicherlich eine Folge der letztjährigen Angriffe auf Webcams mit Standardpasswörtern, welche zu einer Sensibilisierung führten. Die nicht passwortgeschützten Kameras zeigen oftmals Überwachungen von Eingängen, Gebäuden und Räumen. Problematisch wird es hier in Bezug auf den Datenschutz.

Ist Ihre Webcam im Internet auffindbar? Sind damit Personen bestimmbar?

Bei Betrachtung weiterer Protokolle, welche Videosignale übertragen, findet sich das Real-Time- Streaming-Protocol (RTSP). Über 5'100 Streams sind zu finden. In den Stichproben konnten keine Streams gefunden werden, welche nicht durch ein Passwort geschützt waren.

4.4 Web Applikationen

Die konstant hohe Anzahl an Webdiensten bietet weitere Möglichkeiten, Dienste und Geräte genauer zu identifizieren. Eine davon ist das Favicon (favorite icon: Favoriten-Symbol), welches Webseiten auf wiedererkennbare Weise kennzeichnet. Diese Kennzeichnung verwendeten wir bei unserer Inventarisierung. Sie zeigt die Anzahl der meist identifizierten Favicons auf den Hosts (IP-Adressen) an.

Es ist spannend zu sehen, dass die am häufigsten identifizierten Applikationen alle Zugänge zu Administrationsoberflächen von Firewalls (FRITZ!Box, DELL SonicWALL, Thomson), Webseiten Management (Parallel Plesk) und Webkameras sind.

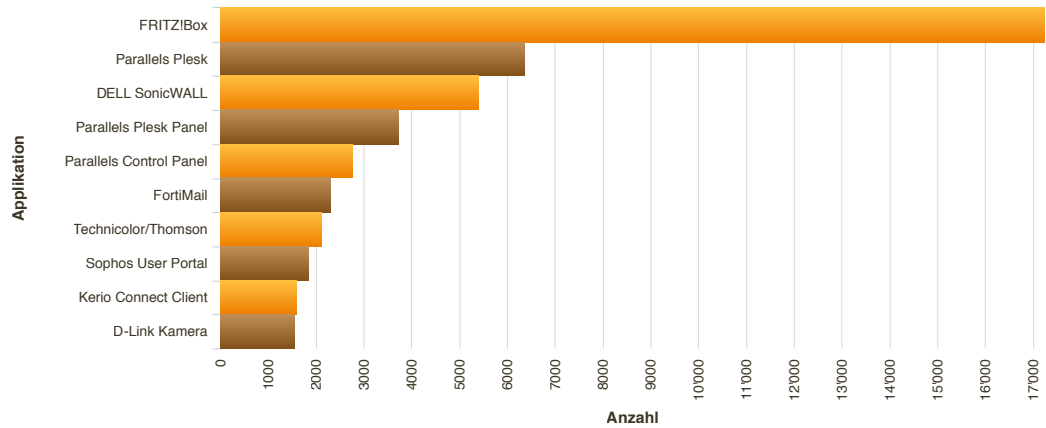


Abbildung 10: Am häufigsten identifizierte Applikationen durch das Favicon

Das meta-Tag «generator» beschreibt das Programm, mit dem die Webseite erstellt wurde. Diese Informationen geben Auskunft über verwendete Programme und dessen Version. Diese Information weist auf Schwachstellen hin und ist daher für Hacker hilfreich.

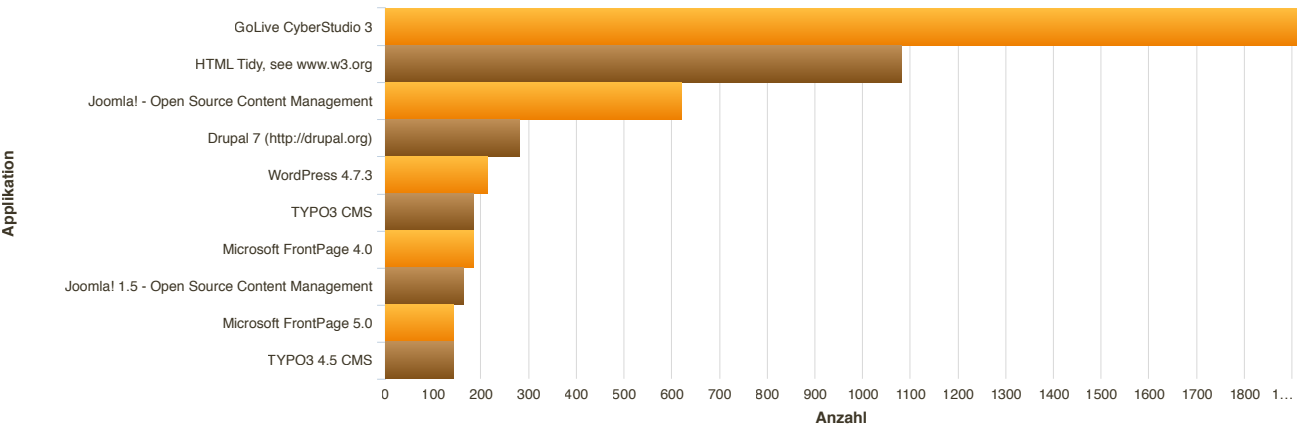


Abbildung 11: Am häufigsten identifizierte Applikationen durch das meta-Tag «generator»

Der am häufigsten eingesetzte Webserver ist Apache. Er ist das Zuhause für PHP-Applikationen. Abbildung 12 zeigt das Verhältnis und die Anzahl der identifizierten PHP-Versionen. Nicht ersichtlich ist die aktuellste PHP-Version, denn PHP 7 gibt diese Information standardmässig nicht preis.

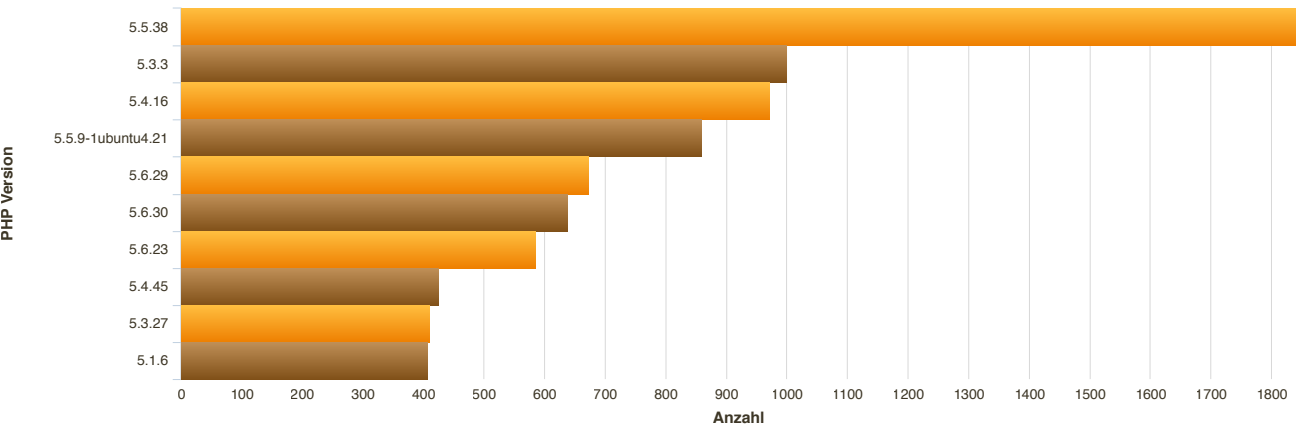


Abbildung 12: Identifizierte PHP Versionen

5. Schwachstellen in Verschlüsselungen

Viele neu bekannt gewordenen Schwachstellen bestehen in Verschlüsselungstechniken wie SSL und TLS, welche für die verschlüsselte Verbindung von Webseiten (HTTPS), E-Mail-Transfer (SMTPS, POP3S, IMAPS), Filetransfer per SFTP, Datenbanken wie Oracle und auch VPN (SSL VPN) Verwendung finden. Die Analyse zeigt, wie sicher verschlüsselte Verbindungen in der Schweiz wirklich sind: Auch eine ungenügende Verschlüsselung lässt den Benutzer im Glauben, dass seine übertragenen Daten vor Einblicken und Veränderungen sicher sind.

99.9 % der erfolgreichen Cyber-Angriffe erfolgen über Schwachstellen, welche seit über einem Jahr bekannt sind. Diese gilt es zu identifizieren und beheben!

5.1 Poodle

Die Poodle («Padding Oracle On Downgraded Legacy Encryption») ist eine «man in the middle» (MITM)-Schwachstelle. Poodle wurde am 14. Oktober 2014 publiziert. 2,5 Jahre danach sind immer noch über 67'000 der knapp 250'000 Verbindungen auf Angriffe anfällig. Dies entspricht 27 % der HTTPS Verbindungen auf Port 443/tcp; lediglich eine bescheidene Verbesserung gegenüber den 35 % im letzten Jahr. Damit ist leider klar aufgezeigt, dass diese Systeme sehr lange nicht oder sogar nie gepatcht werden.

Der Einsatz des HTTPS-Admin-Port (8443/tcp), welcher für die Administration verwendet wird, ist von 9 % auf 17 % angestiegen. Prozentual und absolut gibt es dieses Jahr mehr anfällige Systeme. Eine bedenkliche Entwicklung!

Eine leichte Verbesserung konnten hingegen die E-Mail-Dienste IMAPS (993/tcp), POP3S (995/tcp) und SMTPS (465/tcp) verzeichnen. Dennoch sind über 10 % der E-Mail-Server immer noch angreifbar. Anscheinend werden die E-Mail-Zugangsdaten und die E-Mail-Inhalte als immer noch zu wenig wichtig eingestuft.

OracleS (2484/tcp) und XMPPS (5223/tcp – XMPP, erweiterbares Nachrichten- und Anwesenheitsprotokoll; früher Jabber) fallen dank der kleinen Anzahl aktiver, verschlüsselter Verbindungen nicht ins Gewicht.

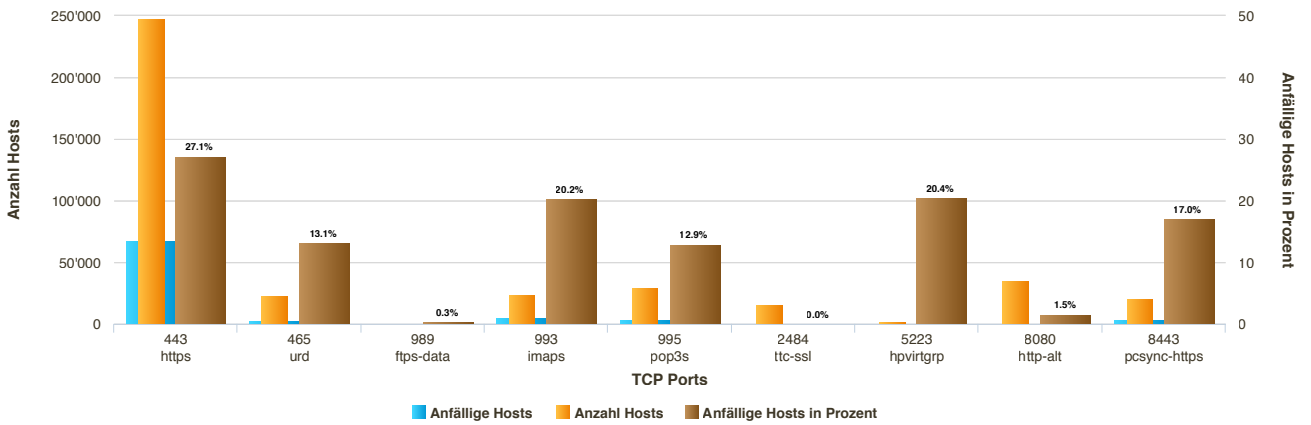


Abbildung 13: Server anfällig auf POODLE

5.2 Logjam

Logjam ist eine Angriffsmethode gegen das Diffie-Hellman-Schlüsselaustausch-Protokoll, welches bei TLS verwendet wird. Es ermöglicht eine «man in the middle» (MITM)-Angriffe indem es ein Herabstufen (downgrade) auf 512-bit export-grade-Verschlüsselung erlaubt. Somit kann ein Angreifer Daten der verschlüsselten Verbindung lesen und modifizieren. Diese Schwachstelle ist mittlerweile nur noch bei ganz wenigen Systemen ausnutzbar. Ein gutes Zeugnis. Es stellt sich die Frage, wieso das Patching hier funktioniert und bei anderen Schwachstellen nicht.

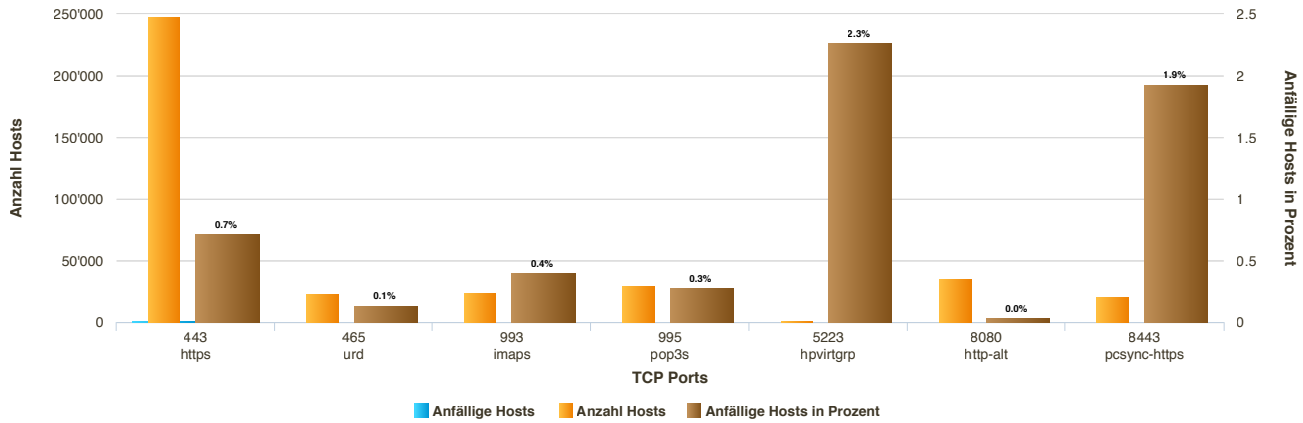


Abbildung 14: Server anfällig auf Logjam

5.3 Freak

FREAK (für Factoring RSA Export Keys) ist eine kryptographische Schwachstelle im SSL- und TLS-Protokoll und wurde im Jahr 2015 bekannt. Wie bei Logjam wird auch hier die historisch bedingte Rückstufung der RSA-Schlüssellänge von nicht mehr als 512 Bits erzwungen. Bei solchen Rückstufungsangriffen müssen Server und Clients diese schwachen Algorithmen unterstützen. Ein Update der verwendeten Client Software, wie Browser, bewahrt nicht davor, Opfer einer solchen Schwachstelle zu werden.

Es zeigt sich dasselbe Bild wie bei Poodle: Bis auf den HTTPS Admin Port (8443/tcp) gab es überall einen kleinen Rückgang der anfälligen Systeme.

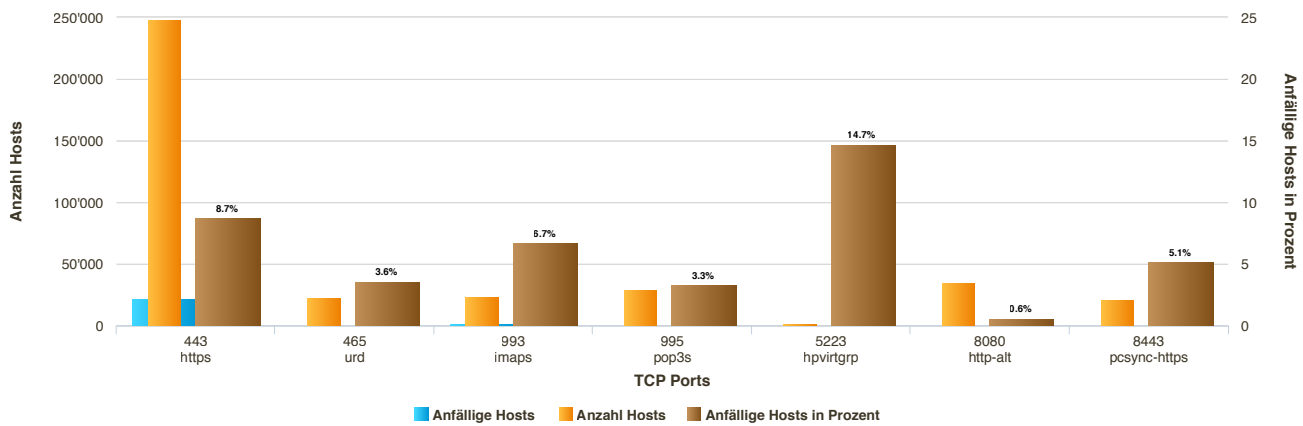


Abbildung 15: Server anfällig auf Freak

5.4 Drown

Bei Bekanntwerden der DROWN-Schwachstelle am 1. März 2016 waren weltweit 33 % der HTTPS Webseiten im Risiko. Bei der DROWN-Angriffe geht es darum, den Private Key über das unsichere SSLv2 Protokoll zu identifizieren. Da oft auf demselben Server oder sogar unternehmensweit das gleiche Zertifikat für verschiedene Protokolle und Dienste Verwendung findet, genügt eine SSLv2 Verbindung, um den Private-Key herauszufinden und damit sichere TLS-Verbindungen mitzuhören und zu manipulieren.

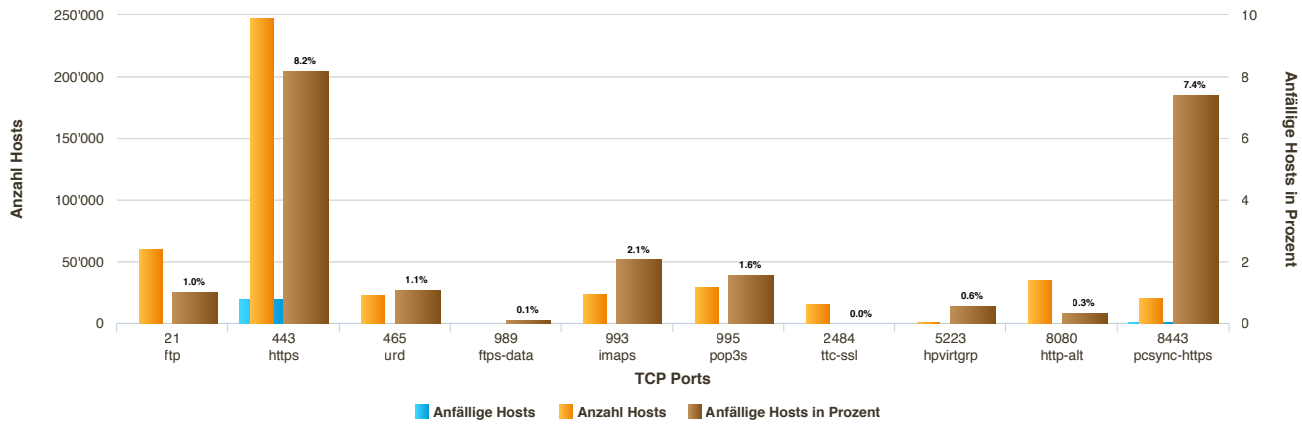


Abbildung 16: Server anfällig auf Drown

5.5 SSL/TLS-CCS Injection

Wie viele der hier beschriebenen TLS-Schwachstellen ist auch diese über eine MITM-Attacke ausnutzbar. Der Angreifer sendet eine entsprechende «ChangeCipherSpec»-Meldung beim TLS-Verbindungsaufbau an beide Verbindungsteilnehmer. Dies hat zur Folge, dass die Länge des «pre master secret key» null wird. Der Angreifer kann die Verbindung entschlüsseln und übertragene Daten manipulieren.

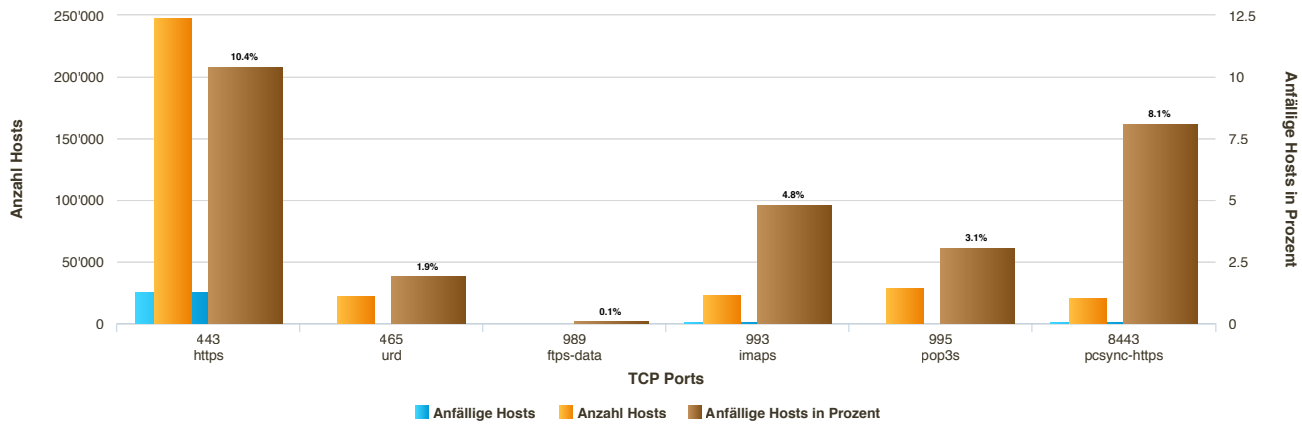


Abbildung 17: Server anfällig auf SSL/TLS-CCS Injection

5.6 Verschlüsselungsstärken

Auch bei Betrachtung der schlechtesten Verschlüsselungsstärke, welche die jeweiligen Services anbieten, gilt in den meisten Fällen: Die Kette ist nur so stark wie ihr schwächstes Glied.

In den beiden Kategorien A und B befinden sich die Verschlüsselungsalgorithmen (z.B. AES) und Schlüssellängen (>2048 bit), welche heute eine sichere Verschlüsselung bieten. In der Kategorie C finden sich Algorithmen wie 3DES und Keys mit DH und RSA 1024 bit. In der Kategorie D kommt bereits DES zum Einsatz und die Kategorien E und F sind heute nicht mehr zu verwenden.

Unter die Kategorien D bis F fallen in der Schweiz 100'000 Services. Unter die besseren Kategorien A bis C fallen 182'000 Services. Ein Drittel davon, 62'000, befinden sich in der besten Kategorie A. Die Verschlüsselungen der Kategorie A werden durch alle aktuellen Browser unterstützt und sind ganz klar zu bevorzugen.

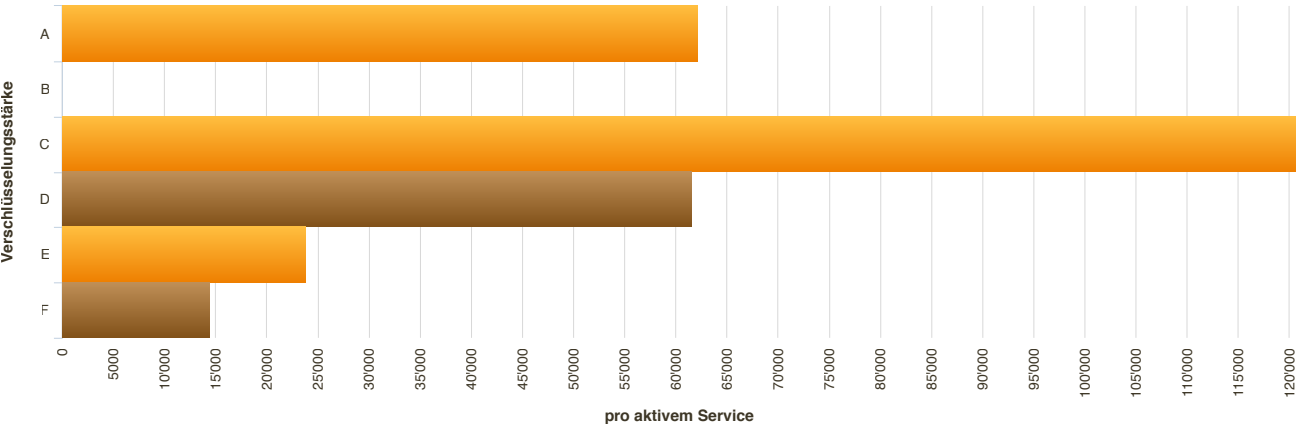


Abbildung 18: Verschlüsselungsstärke pro aktivem Service

Vergleichen wir die Schlüssellängen für RSA bei SSH, sehen wir, dass weniger als ein Drittel auf dem 1024-Bit-Schlüssel basieren. Diese gelten als zu unsicher. Es wird empfohlen, mindestens 2048-Bit-Schlüssel zu verwenden.

Bei den über 20'000 RDP (Remote Desktop) Verbindungen bieten über 8'000 eine ungenügend starke Verschlüsselung durch RC4 40 Bit an.

6. Falschkonfiguration als Schwachstelle (Security Misconfiguration)

Nach der «OWASP Top 10 2017» der erfolgreichen Web-Cyber-Angriffe liegt die Sicherheitsfalschkonfigurationen auf dem Fünften Platz. Dies ist nicht nur bei Webapplikationen, sondern bei allen Internetdiensten der Fall. Gewisse Dienste sollten nicht direkt über das Internet ansprechbar sein, da sie sensitive Informationen preisgeben. Bei anderen Diensten liegt es an deren Spezifikation, dass sie nie sicher sein können.

6.1 FTP-Zugang: Zugang ohne Passwörter

FTP bietet eine einfache und schnelle Art der Datenübertragung im Netzwerk an. Die Sicherheit steht bei der Grundkonfiguration nicht im Vordergrund. Viele Geräte wie NAS (Network Attached Storage) sind einfach zu verwaltende Dateiserver und finden Verwendung in Kleinunternehmen und bei Privatpersonen. Um die Einfachheit des Datenzugriffs zu gewährleisten, konfigurieren sich diese Systeme rudimentär und erlauben mit wenigen Klicks den Zugriff über das Internet. Und schon sind die sensitiven Daten für alle im

Keine oder Standard-Passwörter erlauben Zugriff auf sensitive Informationen!

Internet sichtbar. Es konnten ähnlich viele FTP-Zugänge wie vor einem Jahr gefunden werden. Unsere Prüfung zeigt, dass 3.9 % oder 2'300 aller Logins auf FTP-Server ein anonymes Login erlauben. Das bedeutet: Jeder kann sich dort einloggen. Stichproben zeigen, dass über 10 % dieser frei zugänglichen FTP-Dienste sensitive Daten anbieten. Dies können Backups

ganzer Computer, die gesamte E-Mail-Korrespondenz als Kopie, Buchhaltungs- und Jahresabschlüsse, Kundendaten aus CRM, Offerten, Steuererklärungen, elektronische Bankauszüge, Software bis hin zu der privaten Fotosammlung sein. Zusätzlich zur Problematik, dass Daten veröffentlicht, verändert oder gelöscht werden, ist es oftmals auch möglich, neue Daten für das Sharing hochzuladen. Wo Schreibzugriff erlaubt ist, findet sich Malware in den Verzeichnissen, was bei der Mehrheit der Fall ist. Eine weitere Problematik ist der Datenschutz, welcher sich an der neuen EU-DSGVO ausrichten und auch auf die Schweizer Rechtslage auswirken wird. Finden sich Personendaten auf diesen nicht geschützten Verzeichnissen und kommt es zum Datenabfluss, ist mit hohen Strafzahlungen zu rechnen.

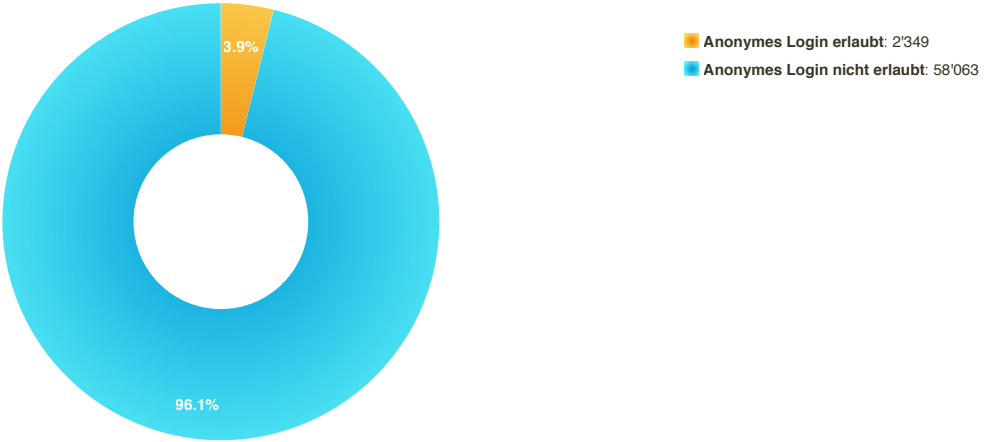


Abbildung 19: FTP mit und ohne anonymem Login

6.2 NTLM: Informationen über das interne Netzwerk

NTLM (NT LAN Manager) ist ein Authentifizierungsverfahren, welches von Microsoft entwickelt wurde. Mit der Windows-Benutzeranmeldung können Dienste wie E-Mail, Web und Telnet mittels NTLM eine Authentifizierung durchführen. Der NTLM-Service erhält Informationen über die DNS- und NetBIOS- Einstellungen. So ist über die Workgroup oder Domäne der Computernamen des Servers bekannt, welcher in der Regel intern verwendete Informationen enthält. Die verschiedenen E-Mail-Dienste weisen diese Informationsfreizügigkeit zwischen 2 % und 9 % auf, jeweils um die 2'000 Systeme der möglichen Hosts. Dies entspricht einer Zunahme im Vergleich zum Vorjahr. Sehr oft beinhalten diese Informationen

den Firmennamen sowie den Servernamen, welcher auf die Art des Servers und des Betriebssystems schliessen lässt. Bei den http- und Telnet-Diensten wurde kein aktives NTLM identifiziert.

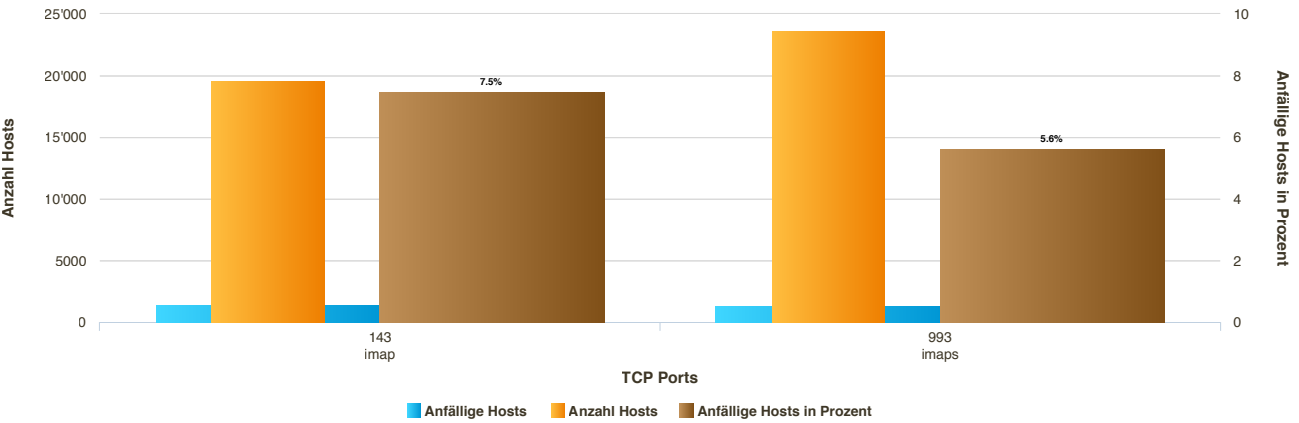


Abbildung 20: IMAP Services mit aktiver NTLM-Authentifizierung

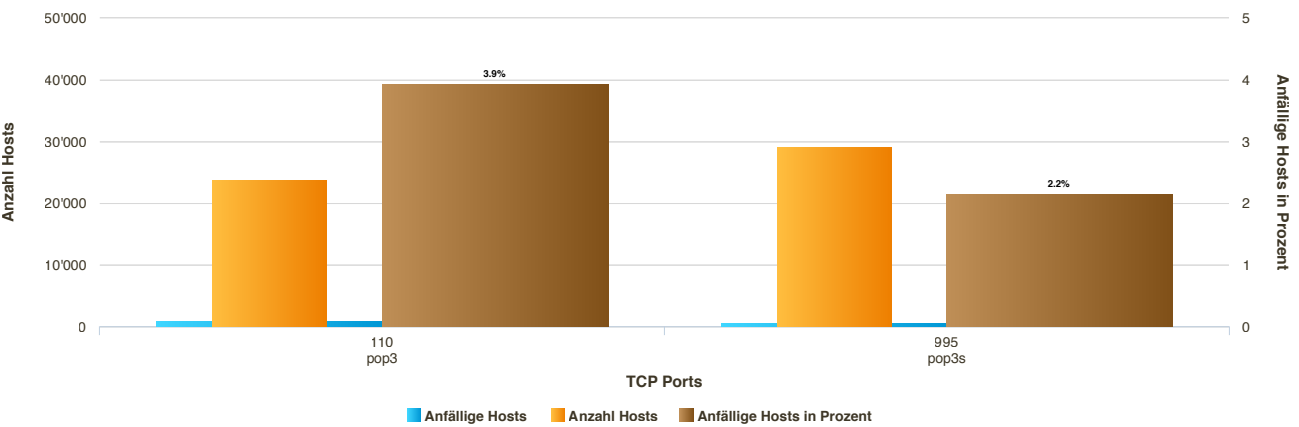


Abbildung 21: POP3 Services mit aktiver NTLM-Authentifizierung

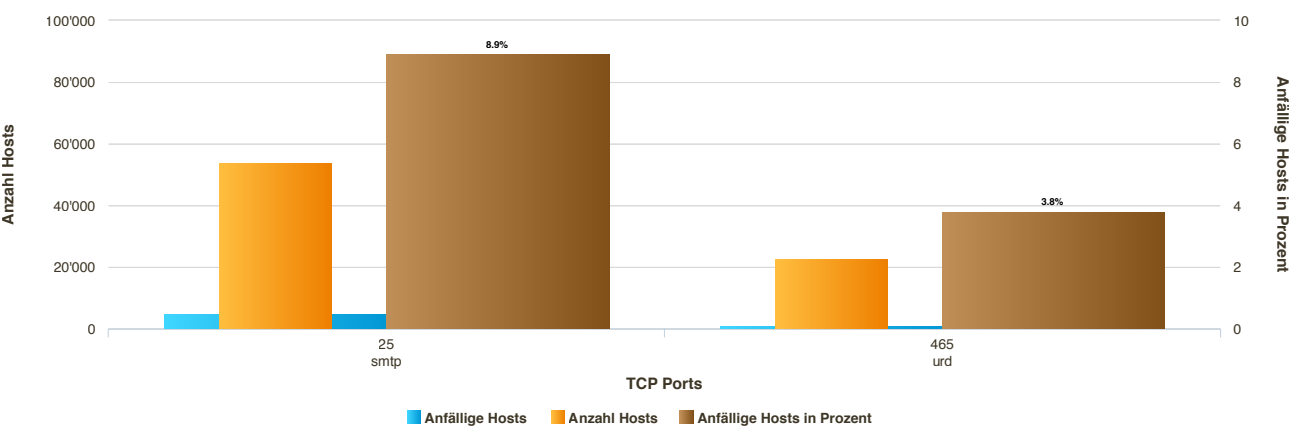


Abbildung 22: SMTP Services mit aktiver NTLM-Authentifizierung

6.3 SMB

Wie bei NTLM werden bei SMB (Server Message Block) Namensauflösungen auf Computer Name, Domain, FQDN etc. ermöglicht. SMB stellt die Datei- und Druckerfreigabe zur Verfügung. Obwohl einige ISPs in der Schweiz den Port 445/tcp für SMB-Verkehr sperren, sind über 9'000 SMB-Dienste erreichbar; 50 % mehr als letztes Jahr und davon sind 3'400 grosszügig mit ihrer Auskunft. Neben den Namen hat man Zugriff auf die freigegebenen Dateien und Drucker, welche durch Benutzername und Passwort geschützt sind. Oftmals sind dies Standard-Zugangsdaten oder sehr einfache Codes. Selbst Microsoft empfiehlt den SMB-Dienst nicht direkt über das Internet verfügbar zu machen.

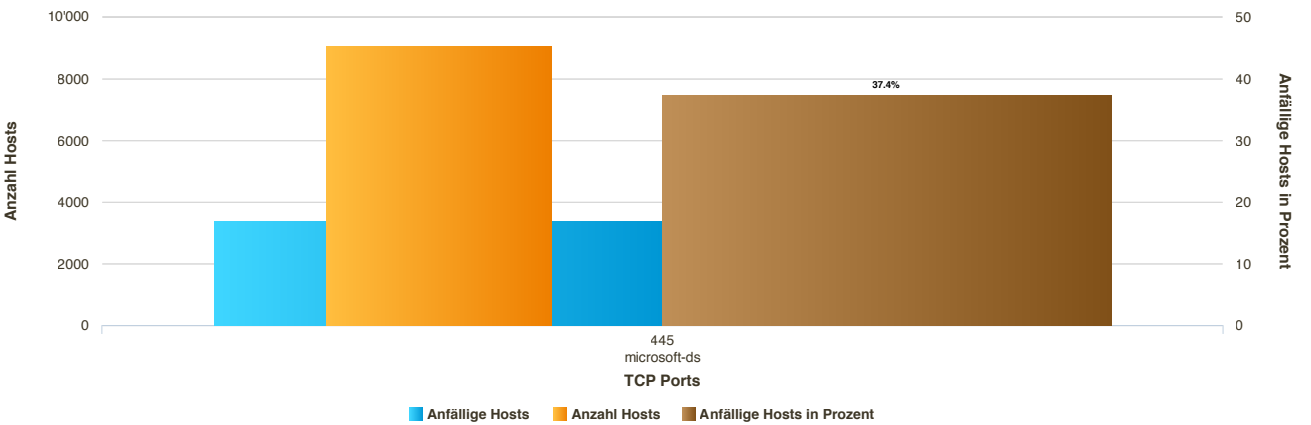


Abbildung 23: Server anfällig auf SMB-Anfragen

6.4 Memcached

Memcached ist ein Cache-Server zum allgemeinen Hinterlegen und Abholen von Daten aus dem Arbeitsspeicher. Er ist auf dem Port 11211/tcp ansprechbar und mit der Info-Abfrage teilt der Server Details über Anzahl Verbindungen, Uptime, Prozess-ID etc. mit. Ein Dienst, welcher nicht direkt im Internet angeboten werden sollte. Es finden sich 21'000 offene Ports in der Schweiz und glücklicherweise geben lediglich 249 (1.2 %) detaillierte Auskunft.



Abbildung 24: Memcached

7. Fazit

Wir werden immer wieder gefragt:

Und nun, was sollten wir tun?

Viele Unternehmungen haben immer noch keine klare IT-Strategie oder die IT-Projekte und IT- Infrastruktur sind nicht mehr überschaubar. Historisches Wachstum führte zu einem Wildwuchs, die Dokumentation litt stark darunter, die Komplexität wuchs in den letzten Jahren und niemand weiss mehr genau, was alles in der IT vorhanden und wie es miteinander verknüpft ist. Eine Überprüfung der IT-Infrastruktur schafft hier Abhilfe.

Viele Firmen neigen dazu, zuerst die bekannten Probleme zu lösen, bevor sie sich an eine Prüfung heranwagen. Der effizientere Weg ist,

zuerst eine Prüfung durchzuführen um anhand der gewonnen, effektiven Informationen die richtigen Entscheidungen effizient treffen zu können.

Genau hier hilft die FST mit ihrer Lösung mit verhältnismässig geringem Aufwand sich einfach und schnell eine Übersicht (Inventar und Zustand) zu verschaffen. Im Zeitalter von Cyber-Kriminalität und -Spionage ist es für den Markterfolg essentiell, eine sichere IT zu betreiben.

7.1 Vulnerability Management

Um die effektiven Schwachstellen in Ihrem Netzwerk zu identifizieren und möglichst rasch zu beheben, empfiehlt sich eine regelmässige Prüfung. Dieser Prozess inklusive Behebung von Schwachstellen nennt sich Vulnerability-Management. Dabei wird in einem ersten Schritt die Infrastruktur inventarisiert – genau so, wie wir es für diesen Bericht über die gesamte Schweizer IT-Landschaft gemacht haben. So können die aktiven Systeme identifiziert werden. Die vertiefte Sicherheitsuntersuchung deckt dann die real existierenden Schwachstellen auf. Diese werden in stufengerechten Reports aufbereitet und priorisiert. Eine klare Anleitung unterstützt Sie anschliessend darin, die Schwachstellen korrekt und effizient zu beheben. Auf diese Weise steigern Sie die Effizienz und Effektivität Ihrer IT und erhöhen die IT-Sicherheit markant. So reduzieren Sie Ihre IT-Risiken und sparen mittel- und langfristig viel Geld.

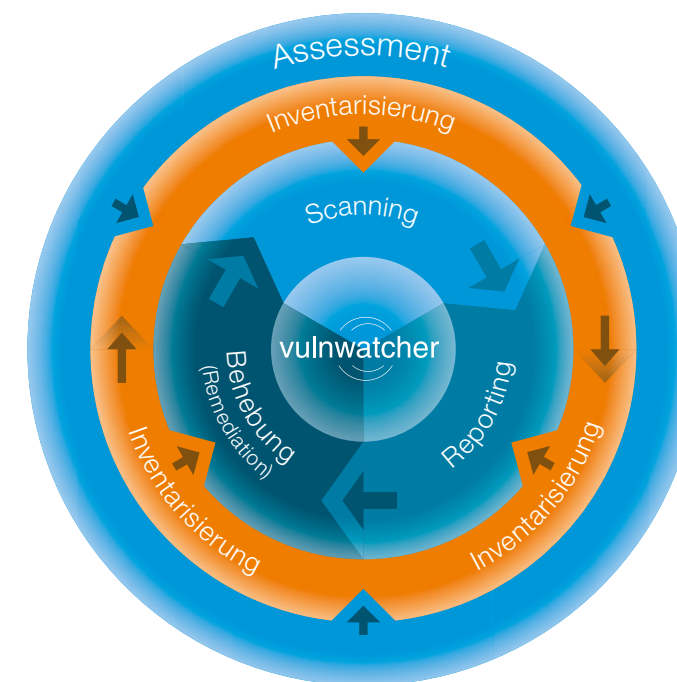


Abbildung 25: Vulnerability-Management-Prozess

7.2 Software-Updates

Regelmässige Updates des Betriebssystems, der Services und der Applikationen sind zwingend notwendig, um Angriffe auf bereits bekannte Schwachstellen abzuwenden. Softwareverteilungslösungen und Patch Management dienen als wertvolle Werkzeuge für solche Updates.

7.3 Firewall richtig konfigurieren

Eine Firewall verringert die Angriffsfläche massgeblich. Nicht benötigte Dienste sollten gar nicht erst vom Internet ansprechbar sein. Wir stellen aber immer wieder fest, dass Firewalls nicht optimal konfiguriert oder Systeme direkt ohne Firewall an öffentliche Netzwerke angeschlossen sind. Betreiber sollten ihre IP-Adressen im Internet regelmässig prüfen – so, wie sie Backups regelmässig durchführen oder Antivirussysteme aktualisieren. Der Inventarisierungs-Dienst der First Security Technology führt solche Überprüfungen in kurzer Zeit durch.

7.4 Verschlüsselung und Passwörter

Passwörter und sensitive Informationen dürfen nie unverschlüsselt übermittelt werden. Unsere Erfahrung zeigt, dass noch immer viele Remote- und Administrationszugänge nicht oder nur schlecht verschlüsselt sind. Aber auch via E-Mail wird oft nicht verschlüsselt kommuniziert. Wir meinen damit nicht nur unverschlüsselte E-Mails, sondern auch die unverschlüsselte Authentifizierung beim Empfangen und Versenden von E-Mails. Passwörter für den E-Mail-Zugang, die in Klartext übermittelt werden, lassen sich sehr einfach abfangen – entsprechend häufig wird dies ausgenutzt.

8. Glossary

8.1 CVSS

Quelle:
<http://de.wikipedia.org/wiki/CVSS>

Das **Common Vulnerability Scoring System** (wörtlich übersetzt: «Gebräuchliches Verwundbarkeitsbewertungssystem»), abgekürzt CVSS, ist ein Industriestandard zur Beschreibung des Schweregrades von Sicherheitslücken in Computer-Systemen. Im CVSS werden Sicherheitslücken nach verschiedenen Kriterien, sogenannten Metrics, bewertet und miteinander verglichen, so dass eine Prioritätenliste für Gegenmassnahmen erstellt werden kann. CVSS ist selbst kein System zur Warnung vor Sicherheitslücken sondern ein Standard, um verschiedene Beschreibungs- und Messsysteme miteinander kompatibel und allgemein verständlich zu machen.

Dabei bedeutet 0 kein Risiko und 10 ist der maximale Wert und stellt eine bedrohliche Schwachstelle dar.

8.2 CVE Datenbank

Quelle:
http://de.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

Common Vulnerabilities and Exposures (CVE) ist ein Industriestandard, dessen Ziel die Einführung einer einheitlichen Namenskonvention für Sicherheitslücken und andere Schwachstellen in Computersystemen ist. Mehrfachbenennung gleicher Gefahren durch verschiedene Unternehmen und Institutionen werden um eine laufende Nummer (z. B. CVE-2006-3086) ergänzt, um eine eindeutige Identifizierung der Schwachstelle zu gewährleisten. Dadurch ist ein reibungsloser Informationsaustausch zwischen den verschiedenen Datenbanken einzelner Hersteller möglich.

Die Liste der Common Vulnerabilities and Exposures wird von der MITRE Corporation in Zusammenarbeit mit Sicherheitsexperten, Bildungseinrichtungen, Behörden und Herstellern von Sicherheitssoftware (wie z.B. Antivirenprogramme) verwaltet.

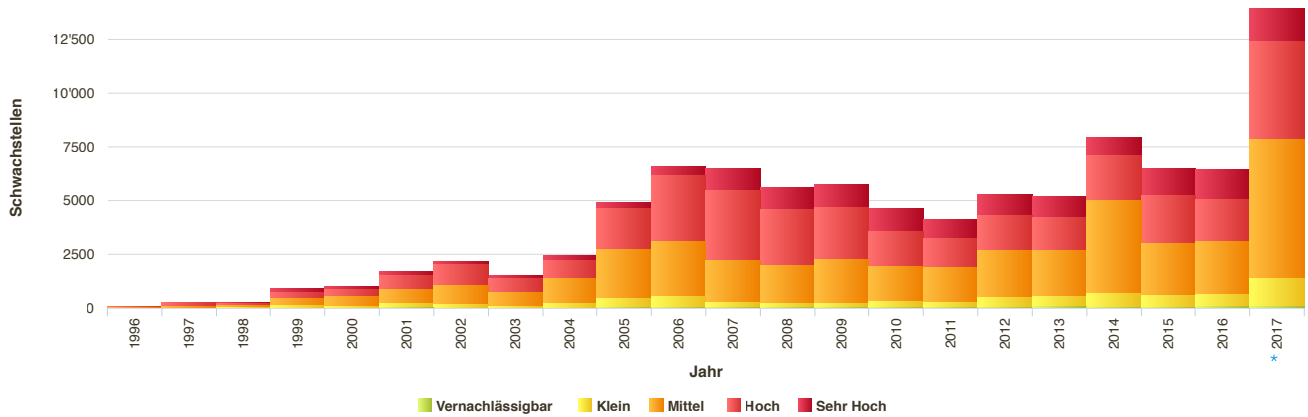


Abbildung 26: neue Schwachstellen pro Jahr in der CVE-Datenbank mit Schweregrad

* Für 2017 sind die Zahlen linear vorberechnet worden. Durch die vielen Leaks Anfang Jahr ergibt das eine Verdoppelung gegenüber den Vorjahren. Wir hoffen, dass es nicht so viele sein werden.

8.3 Port

(Liste mit am meisten
verwendeten Diensten)

Port	Protokoll	Name
21	TCP	FTP
22	TCP	SSH
23	TCP	TELNET
25	TCP	SMTP
50	TCP	IKE (VPN)
53	TCP	DNS
69	TCP	TFTP
80	TCP	HTTP
110	TCP	POP3
123	TCP	NTP
137	TCP	NETBIOS

(Liste mit am meisten
verwendeten Diensten)

Port	Protokoll	Name
139	TCP	NETBIOS
143	TCP	IMAP
161	TCP	SNMP
389	TCP	LDAP
443	TCP	HTTPS
445	TCP	MICROSOFT-DS (SMB)
451	TCP	SFS-SMP-NET
465	TCP	SMTPS
515	TCP	LPD
547	TCP	DHCP
554	TCP	REAL TIME STREAMING PROTOCOL (RTSP)
631	TCP	INTERNET PRINTING PROTOCOL (IPP)
989	TCP	FTPS
993	TCP	IMAPS
995	TCP	POP3S
1433	TCP	MSSQL
1521	TCP	ORACLE
1701	TCP	VPN
1723	TCP	PPTP
2082	TCP	CPANEL
2483	TCP	ORACLE
2484	TCP	ORACLES
3306	TCP	MYSQL
3389	TCP	RDP
4500	TCP	VPN (IKE NAT-T)
5000	TCP	UPNP
5060	TCP	SIP
5222	TCP	XMPP
5223	TCP	XMPPS
5432	TCP	POSTGRESSQL
5900	TCP	VNC
6379	TCP	REDIS
7547	TCP	D1000 MODEM
8080	TCP	HTTP ADMIN
8443	TCP	HTTPS ADMIN
9100	TCP	JETDIRECT
9200	TCP	ELASTICSEARCH
11211	TCP	(MEMCACHED)
27017	TCP	MONGODB
27018	TCP	MONGODB (SHARDSVR)
27019	TCP	MONGODB (CONFIGSVR)
28017	TCP	MONGODB (WEB STATUS PAGE)
28019	TCP	MONGODB (CONFIGSVR) (WEB STATUS PAGE)
50060	TCP	HADOOP (TASKTRACKERS)
50070	TCP	HADOOP (NAMENODE)

Die Namen der Ports sind durch den Standard gegeben. Es können auf den TCP Ports auch andere Services aktiv sein. Die Auswertungen auf den Produkten basieren auf den Bannern und nicht auf den TCP Ports.

8.4 Schwachstelle

Eine Schwachstelle ist eine Sicherheitslücke in der IT-Umgebung.

8.5 Vulnerability

Siehe Schwachstelle.

8.6 Schweizer Cyberspace

In diesem Report sprechen wir vom Schweizer Internet und verstehen dabei die öffentlichen IP-Adressen, die mit einer Schweizer Postadresse bei «RIPE NCC» eingetragen sind. Das Réseaux IP Européens Network Coordination Centre (RIPE NCC) ist eine Regional Internet Registry (RIR), zuständig für die Vergabe von IP-Adressbereichen und AS-Nummern in Europa, dem Nahen Osten und Zentralasien.

9. Disclaimer

Kein Teil dieser Dokumentation darf ohne schriftliche Zusage der First Security Technology AG vervielfältigt oder verbreitet werden. Erlaubt ist einzig das Zitieren aus dem Swiss Vulnerability Report 2017 mit Angabe der Quelle und dem Verweis auf die Urheberschaft durch die First Security Technology AG.

Wir sind bestrebt, zutreffende, fehlerfreie und präzise Aussagen zu unseren Untersuchungen und den Ergebnissen dieser Studie zu machen. Dennoch kann die First Security Technology AG keine Gewähr für die Richtigkeit und Aktualität der hier aufgeführten Angaben, Aussagen, Daten, Darstellungen und Tabellen bieten.

Wir übernehmen keinerlei Haftung für Dispositionen, Massnahmen und Entscheidungen oder den Einkauf von IT-Systemen jeglicher Art (Hard- oder Software), die aufgrund der hier aufgeführten Angaben getroffen werden. Wir weisen darauf hin, dass die Genauigkeit der System- und Dienste-Erkennung unter anderem davon abhängt, wie viele Informationen der untersuchte Host oder Service preisgibt. Eine Einschränkung der Informationen kann zu Ungenauigkeiten in den aufgeführten Statistiken führen.

First Security Technology AG

it security swiss made

First Security ist der führende Schweizer Hersteller von IT-Schwachstellen-Analysesystemen.

VulnWatcher – Swiss Made Vulnerability Management prüft als webbasierte Standard-Software die gesamte IT-Infrastruktur von Unternehmen in einem zyklischen Prozess regelmässig auf Risiken und Schwachstellen. Sicherheitslücken werden sofort und zuverlässig erkannt, klassifiziert, bedarfs- und stufengerecht rapportiert und deren Beseitigung überwacht. First Security stärkt die IT-Compliance und erhöht die IT-Sicherheit mess und kontrollierbar.

Weitere Informationen <http://www.first-security.com>

