First Security Technology

Austrian Vulnerability Report 2015

Pascal Mittner CEO
Allon Moritz CTO

Chur, 19. Februar 2015

Gestaltung: Hü7 Design AG, www.hue7.ch
Titelbild: Schloss Anif, Österreich
«Anif castle», © dzain – Fotolia

First Security Technology

Austrian Vulnerability Report 2015

Pascal Mittner CEO
Allon Moritz CTO

Chur, 19. Februar 2015

Inhaltsverzeichnis

1. Management Summary

Die First Security Technology AG (FST) hat erstmals einen Austrian-Vulnerability-Report (AVR) verfasst. Nach bereits zweimaliger Durchführung des Swiss Vulnerability Reports, der grossen Resonanz in der Schweiz und dem Bedürfnis über das Wissen von IT-Schwachstellen in Österreich bietet Ihnen dieser Bericht einige sehr interessante Einblicke.

Für diesen Bericht unterzogen wir die Österreich zugeteilten IP-Bereiche einer Prüfung. Mit einer verteilten Scan-Node-Architektur überprüften wir über 13 Millionen IP-Adressen. Diese IP-Adressen sind gemäss Who-is-Abfragen auf Österreichische Postadressen eingetragen. Beim Verbindungsaufbau werden Informationen über die antwortende Applikation und deren Version zurückgeliefert. Zudem lassen sich Rückschlüsse auf das Betriebssystem ziehen und es kann häufig auch dessen Version eindeutig identifiziert werden.

Unsere Inventarisierung ermittelte über 7'500 verschiedene Produkte, die über IP-Adressen ansprechbar sind. Diese verglichen wir mit der CVE-Datenbank (Common Vulnerabilities and Exposures), die über 61'000 Schwachstellen kennt. So liessen sich die Produkte auf mögliche Schwachstellen prüfen. Der Bericht fasst diese Informationen zusammen und reichert sie mit interessanten Erkenntnissen an, die sich daraus gewinnen liessen.

Als Resultat zeigt der AVR in Zahlen die potenziellen Schwachstellen von Systemen auf, die in Österreich erreichbar sind. Der Fokus liegt dabei auf den 28 am meisten verwendeten Ports. Dabei wurden über 10 Millionen potenzielle Schwachstellen identifiziert.

Der Austrian Vulnerability Report 2015 gibt unter anderem Auskunft über:

- die Zahl der ans Internet angeschlossenen aktiven IP-Adressen;
- die Anzahl der 10 am häufigsten verwendeten Betriebssysteme;
- die Anzahl der verschiedenen Versionen eines Betriebssystems;
- die Art und die Zahl der aktiven Ports im Internet;
- die Art und die Häufigkeit der eingesetzten Internetdienste;
- die Anzahl Schwachstellen bezogen auf Hersteller, Produkte und Versionen sowie im Verhältnis zur Anzahl Hosts;
- die Anzahl Schwachstellen bezogen auf die Ports;

Der Austrian Vulnerability Report liefert bemerkenswerte Einblicke in die Österreichische IT-Landschaft. Die Ergebnisse des Reports können dazu beitragen, Entscheidungsträger aus Wirtschaft und IT dafür zu sensibilisieren, die Sicherheitspolitik in der eigenen IT zu überprüfen. Sie liefern zudem erste Anhaltspunkte, wo sich Schwachstellen und Sicherheitslücken besonders wirksam und mit relativ wenig Aufwand schnell schliessen lassen.

2. Vorwort

Manfred Holzbach
Geschäftsführender Vorstand
Zentrum für sichere Informationstechnologie – Austria (A-SIT)
www.a-sit.at

Liebe Leserinnen, liebe Leser,

Wer wird das Match Bequemlichkeit gegen Sicherheit gewinnen? Können wir vielleicht doch beides haben? Bequemes spüren wir und das ist sehr angenehm. Ein Tipp auf den Touch Screen und schon haben wir was wir wollen. Ab in die Cloud und wir brauchen uns um nichts mehr zu kümmern? Die Daten sind da wenn wir sie anfordern, die Programme sind auf dem letzten Stand und Backups entstehen quasi von selbst. Wer sieht unsere Informationen sonst noch? Wissen wir nicht.

Sicherheit dagegen herrscht dann, wenn nichts passiert. Das ist gar nicht sexy. Wir empfinden so gut wie nichts dabei, nur den Aufwand den wir damit haben. Geht das dann nicht auch billiger? Gefühlte Sicherheit manifestiert sich erst, wenn sie weg ist und dann wollen wir sie mit allen Mitteln wiedererlangen.

Jeder, der sich mit IT-Sicherheit befasst kennt diese Problematik. So ist zur Zeit etwa der unaufhaltsame Trend zu «Bring Your Own Device» eine der grössten Herausforderungen in diesem Zusammenhang.

Was haben uns die Vorfälle und Leaks der letzten Zeit gezeigt? Schadensereignisse oder gefährliche Situationen können auch sehr selten oder zum ersten Mal wider alle Vorhersagen auftreten: ein extremer Tsunami, der ein Kernkraftwerk zerstört. Eine Drohne über dem Weissen Haus, gelenkt von einem betrunkenen Geheimdienstmitarbeiter (wenn man den Medien glauben darf). Ein NSA Mitarbeiter erzählt aus seinem Job. Da stösst dann die klassische Risikoanalyse an die Grenze ihrer Aussagekraft. Als «Schwarze Schwäne» hat der Autor und Börsenhändler Nassim Nicholas Taleb solche Ereignisse bezeichnet: sehr unwahrscheinlich, völlig überraschend und nachher einfach erklärbar. Begegnen können wir ihnen, indem unsere Systeme und Verhaltensweisen so etwas grundsätzlich aushalten können. Dann können wir davon auch für die Zukunft profitieren.

Der vorliegende Vulnerability Report hilft zu erkennen, ob und inwieweit unsere Systeme und in der Konsequenz unsere eigene Einstellung zur Sicherheit verwundbar sind. Es geht dabei nicht um konkrete und gezielte Schwachstellen, sondern um allgemeine Klassen von Verwundbarkeiten, die ein Potenzial für Schadensereignisse darstellen. Auch für solche, die kaum wahrscheinlich sind oder bislang nur theoretisch existieren.

Das soll uns motivieren, unsere Hausaufgaben in Entwicklung und Betrieb sicherer IT noch besser zu machen. Deren Grundzüge sind im Wesentlichen schon lange bekannt. Auch wenn sich die Technologien und Möglichkeiten dramatisch weiterentwickeln – Fehler, Versäumnisse und strukturelle Schwachstellen verändern sich nur langsam. Sie wurzeln in der Schwierigkeit, immer wieder den Break-Even zwischen steigendem Aufwand und steigendem Risiko zu ermitteln. Ersteren kann man gut errechnen, zweiteres ist immer eine mehr oder weniger zuverlässige Wahrscheinlichkeitsschätzung. Dazu kommt die nach wie vor ausbaufähige Awareness über die vitale Bedeutung der IT-Systeme und die verbreitete Illusion, dass die eigene Organisation gar nicht so attraktiv für Angreifer ist. Etwa bei nicht wenigen KMU, welche in ihrer Gesamtheit aber einen Grossteil der österreichischen Wirtschaft ausmachen und deren Daten nicht selten einen extrem hohen Wert darstellen. Und da ist auch die Bequemlichkeit, die sich immer wieder gerne vor die Sicherheit drängt…

Eine wichtige Aufgabe von A-SIT ist es, hier zur breiten Awareness beizutragen, deshalb engagieren wir uns u.a. bei der Redaktion des österreichischen IKT-Sicherheitsportals www.onlinesicherheit.gv.at und des österreichischen Informationssicherheitshandbuchs. Studien und Analysen wie der vorliegende Report sind für unsere Arbeiten eine wichtige Informationsbasis.

Nach diesen Gedanken wünsche ich Ihnen nützliche Erkenntnisse aus der Lektüre des Vulnerability Report, und die Motivation zur Umsetzung.

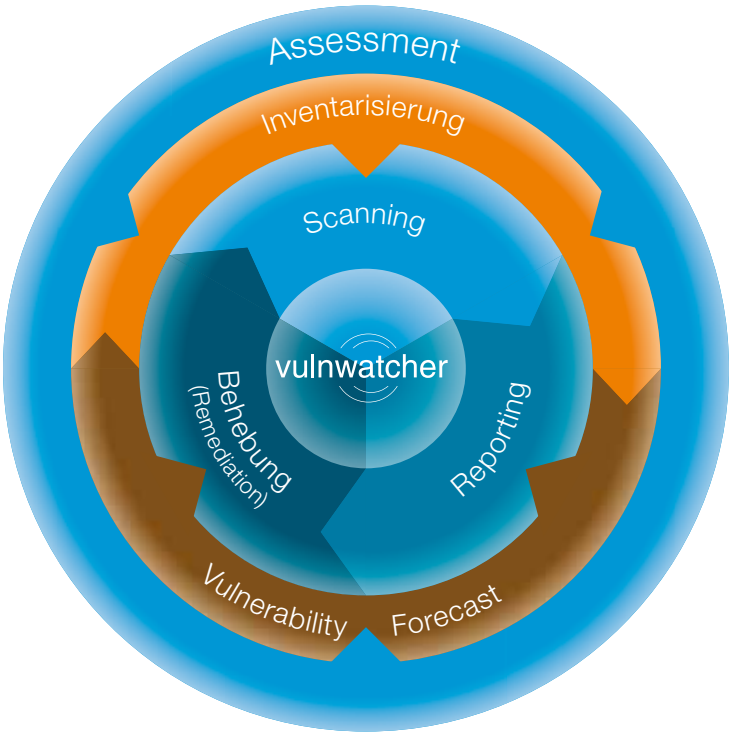
3. Einführung

3.1 Einleitung

Die First Security Technology AG (FST) gehört seit Jahren zu den führenden Herstellern von Schwachstellenanalyse-Software im deutschsprachigen Raum. Zu unseren Kunden zählen kleine, mittlere und grosse Unternehmen in der ganzen Schweiz und im grenznahen Ausland. Auf der Grundlage dieser ausgewiesenen Kompetenz entstand unsere Idee, einen Swiss Vulnerability Report (SVR) zu erstellen. Durch unsere verstärkte Tätigkeit in Österreich, erscheint nun auch der erste Austrian Vulnerability Report (AVR). Auch Österreich soll von dem Wissen über Schwachstellen der Systeme in Ihrem Internet profitieren.

Mit der Schweiz assoziiert man unter anderem Qualität. Verfügbarkeit, Vertraulichkeit und Integrität bilden die Eckpfeiler der IT-Sicherheit. Unsere Mission ist es, die Qualität der IT-Infrastruktur in Bezug auf diese Eckpfeiler zu verbessern. Die Sicherheit von Österreich, ihren Firmen und der Bevölkerung ist uns wichtig. Cybercrime, Malware und Überwachung wecken aktuell vielerorts Ängste. Wir erachten es als unabdingbar, sichere IT-Systeme zu verwenden, um Menschen und Daten nachhaltig zu schützen.

Der AVR zeigt in Zahlen die potenziellen Schwachstellen von Systemen auf, die im Österreichischen Internet erreichbar sind. Wir fokussieren uns auf die 28 am meisten verwendeten Dienste. Indem wir einen aktiven Port identifizieren, erhalten wir oft auch Informationen zum verwendeten Betriebssystem, zu der Applikation und deren Version. Diese Informationen vergleichen wir mit unserer Schwachstellendatenbank, wodurch wir Aussagen zu möglichen Schwachstellen machen können. Wir nennen das Erkennen aktiver Systeme im Netzwerk «Inventarisieren». Die potenziellen Gefährdungen zeigt unsere Schwachstellenvorhersage (Vulnerability Forecast) auf, indem sie einen Zusammenhang zwischen den Schwachstellen und den erkannten Versionen von Betriebssystem und Applikationen herstellt. Inventarisierung und Vulnerability Forecast sind Teilprozesse des Vulnerability Managements. Ein professionelles Vulnerability Management geht noch viel weiter. Die Prozesse Security Scans, Reporting und Behebung bilden den Kern des Vulnerability Managements. Mehr Details über ein ganzheitliches Vulnerability Management finden Sie auf unserer Webseite www.first-security.at



[1] www.sans.org/critical-security-controls/

Die Inventarisierung von autorisierter und nicht autorisierter Hard- und Software belegt die beiden Spitzenplätze derjenigen Themen, die IT-Verantwortliche am meisten beschäftigen (SANS Top 20 Critical Security Controls [1]). Auch im Vulnerability-Management-Prozess spielt die Inventarisierung eine zentrale Rolle. Um die Systeme im eigenen Netzwerk einer tief gehenden Security-Prüfung zu unterziehen, ist eine Identifizierung entscheidend. Auswertungen des Einsatzes von Betriebssystemen, Netzwerkgeräten, Applikationen und ihren verschiedenen Versionen bis hin zu Geräten wie Druckern widerspiegeln den Istzustand des Netzwerks. Die FST hilft ihren Kunden, den Zustand der Systeme in ihrem Netzwerk zu kennen und zu erfahren, welche Systeme von aussen erreichbar sind. Diese Inventarisierung inklusive Vulnerability Forecast führen wir mit der Lösung VulnWatcher einfach, schnell und lizenzunabhängig durch. Kontaktieren Sie uns, damit auch Sie wissen, welche Informationen Ihre IT-Infrastruktur nach aussen preisgibt.

3.2 Technische Details zur Prüfung

Eine verteilte Scan-Node-Architektur führt eine Inventarisierung, bewusst über mehrere Tage verteilt, bei über 13 Millionen IP-Adressen durch. Diese IP-Adressen sind gemäss Who-is-Who-Abfragen auf Österreichische Postadressen eingetragen.

Bei einer Verbindung zu einem aktiven Port werden oftmals Informationen über die Applikation und ihre Version mitgeliefert. So 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.

Die gewonnenen Informationen verglichen wir mit der CVE-Datenbank (Common Vulnerabilities and Exposures), um sie auf mögliche Schwachstellen zu prüfen. Der Bericht fasst diese Informationen zusammen und reichert sie mit interessanten Erkenntnissen an, die sich daraus gewinnen liessen. Die Herausforderung unserer Aufgabe lag neben der Scantechnologie darin, die Resultate korrekt auszuwerten und darzustellen.

Die hier aufgedeckten Schwachstellen stellen potenzielle Gefahren dar, die ausschliesslich auf Fehlern der Software beruhen. Andere Risiken und Falschkonfigurationen, wie zum Beispiel die Verwendung von Standardpasswörtern, werden bei dieser Studie nicht berücksichtigt.

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 IPS (Intrusion-Prävention-Systemen). 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. Aus diesen und weiteren Gründen sprechen wir stets von «potenziellen» Schwachstellen. Dieser Report zeigt in Bezug auf Softwareschwachstellen das Worst Case Szenario. Konfiguration- und Prozess-Schwachstellen kommen zu den hier gezeigten Schwachstellen noch dazu.

3.3 Rechtliches

Aus rechtlichen Gründen darf ein aktiver Security Scan, der tief in ein IT-System vordringt, nicht ohne Einwilligung der Besitzer und Betreiber durchgeführt werden. Wir haben die rechtlich unproblematische Methode angewendet: Wir werteten die öffentlichen Informationen zu Systemen und Versionen aus, die sich ohne Hacking-Techniken erhalten lassen, und inventarisierten sie. Ebenso unproblematisch ist der anschliessende Vergleich mit einer Schwachstellendatenbank.

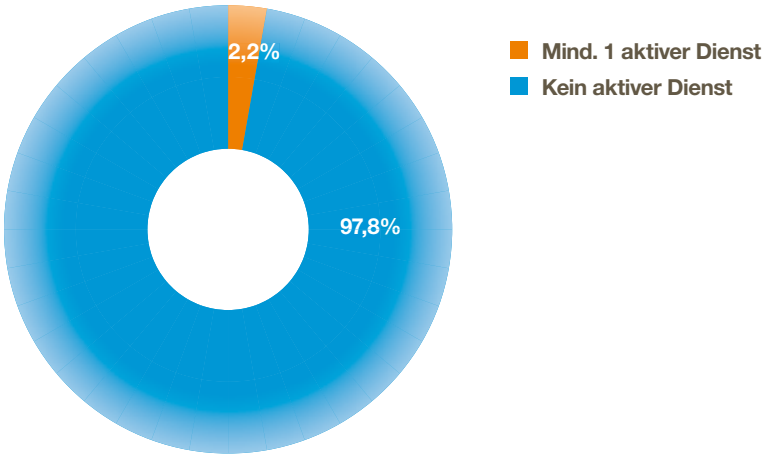
4. Inventarisierung

292’845
Hosts gefunden

577’242
Dienste gefunden

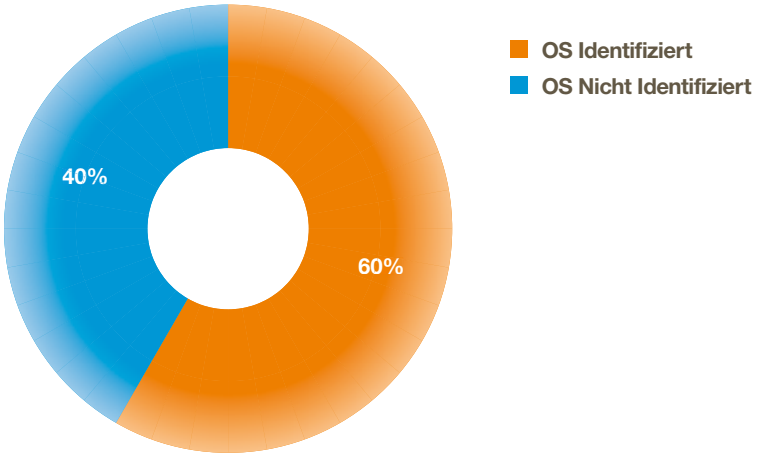
1: Aktive Hosts

Die Prüfung, wie sie in der Einleitung beschrieben wurde, fand bei über 292’000 IP-Adressen mindestens einen aktiven Dienst. Dies sind 2,2% der registrierten Österreichischen IP-Adressen.



2: In Österreich verfügbare Internet IP-Adressen mit aktiven Diensten

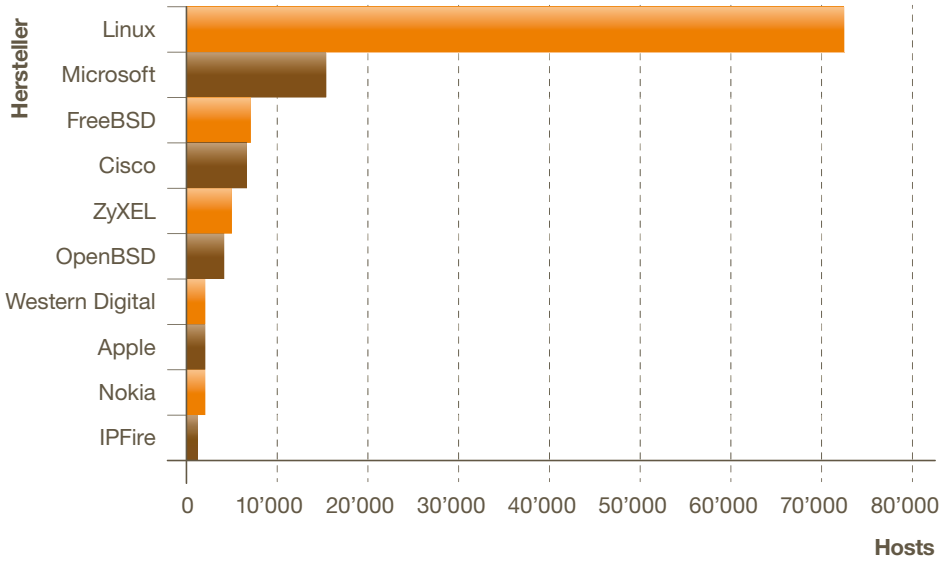
Es ist nicht immer möglich, das Betriebssystem und die Version von aktiven IP-Adressen zu identifizieren. Bei über 175’000 dies entspricht 60% aller aktiven IP-Adressen liess sich das Betriebssystem eindeutig ermitteln. Bei 40% der Systeme war eine eindeutige Bestimmung mit der Technik unter Punkt 3.2 beschrieben, nicht möglich.



3: Identifizierte und nicht identifizierte Betriebssysteme

4.1 Hersteller von Betriebssystemen

Abbildung 4 verdeutlicht die ausserordentlich starke Verbreitung von Linux auf Server-Seite und Netzwerkkomponenten. Gründe für diese Dominanz sind die gute Performance, die hohe Flexibilität, tiefe Lizenzkosten und das Image als sicheres Betriebssystem. Ebenfalls auf Linux basierend ist Western Digital, welches mit einem embedded Linux-System eine Cloud Lösung für Heimanwender bietet. Die Open Source Firewall IPFire basiert auch auf Linux.

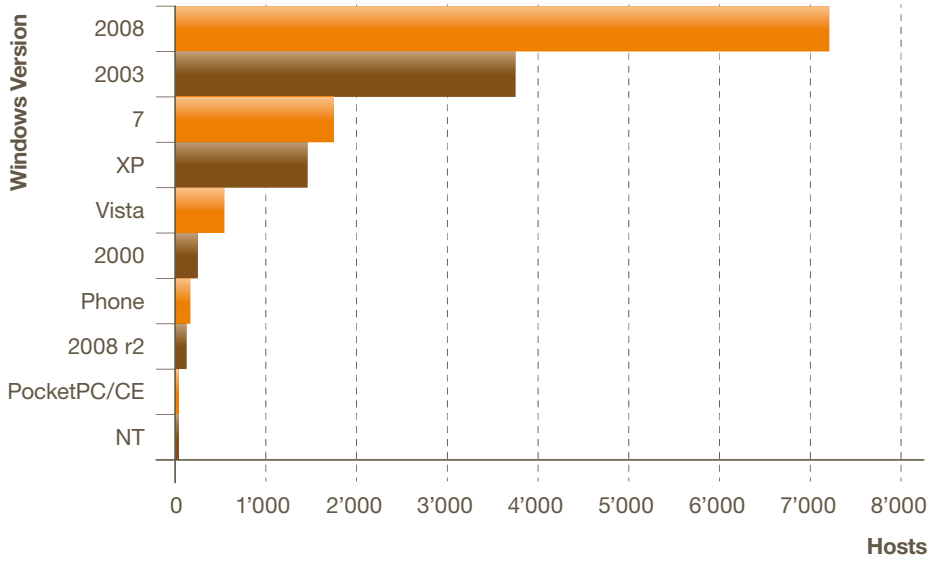


4: Anzahl der Betriebssysteme im Internet in Österreich erreichbar, aufgeteilt nach Herstellern (Linux/BSD sind keine Hersteller, werden in diesem Report aber so behandelt)

4.2 Windows Versionen

Insgesamt wurden über 15'000 Betriebssysteme von Microsoft identifiziert. Den grössten Anteil der Serverversionen machen Windows 2003 und 2008 aus. Über 3'700 Desktop-Betriebssysteme mit den Versionen Windows XP, Vista oder 7 Services bieten sich direkt im Internet an. Für über 1'600 Windows XP, 2000 und NT besteht kein Support mehr durch Microsoft. Dies bedeutet, dass diese Systeme nicht zuverlässig geschützt und daher anfällig für Bedrohungen sind.

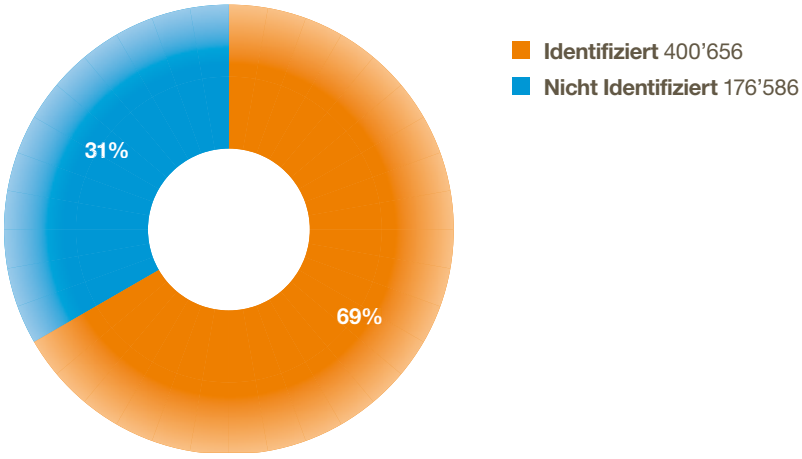
Über 1'600 Windows-Systeme, die nicht mehr vom Hersteller unterstützt werden, sind aus dem Internet erreichbar.



5: Aufteilung der Windows-Versionen

4.3 Ports und Dienste

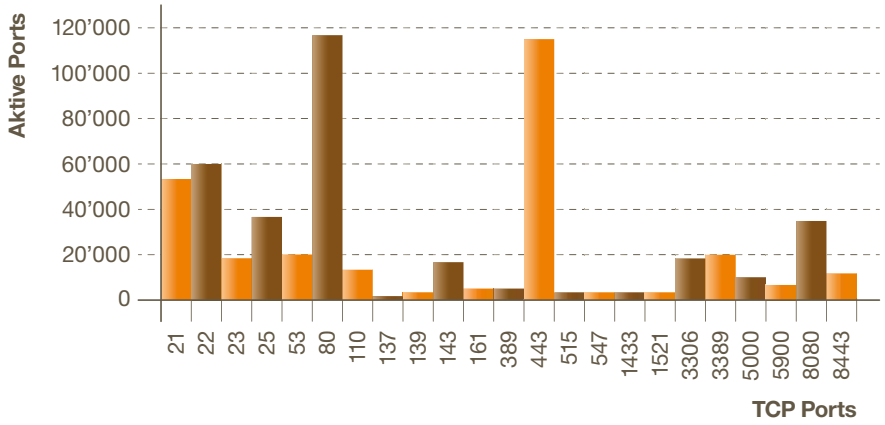
Die fast 13 Millionen IP-Adressen in Österreich wurden auf die 28 Dienste, die statistisch am häufigsten verwendet werden, überprüft. Dabei entdeckten wir über 577'000 aktive Dienste. 69% dieser Dienste gaben das Produkt und die Version der Applikation preis.



6: Verhältnis von identifizierten zu nicht identifizierten Produkten der aktiven Dienste

Abbildung 7 zeigt die Verteilung der identifizierten Ports. Weitaus am meisten kommt HTTP und HTTPS zum Einsatz. SSH und FTP sind ebenfalls gut vertreten. Negativ auffällig sind die über 17'000 Telnet Dienste. Unverschlüsselte Verbindungen zu Firewalls, Routern, Switches, Printern, Webcams beherbergen ein sehr grosses Risiko für das Mithören der Login Details. Über 20'000 Microsoft Terminal Services (RDP) und 6'000 VNC Dienste sind direkt aus dem Internet ansprechbar. Nach Möglichkeit sollten Remotezugriffe nur über VPN oder anderweitig geschützte Verbindungen erlaubt sein. Bei Datenbanken stellt sich auch die Frage, in wie weit diese aus dem Internet direkt erreichbar sein sollten. Über 25'000 MySQL, MSSQL und Oracle Datenbanken sind sichtbar.

Über 26'000 Remote Services, 17'000 unverschlüsselte Telnet Services und 25'000 Datenbanken sind im Österreichischen Internet öffentlich erreichbar.



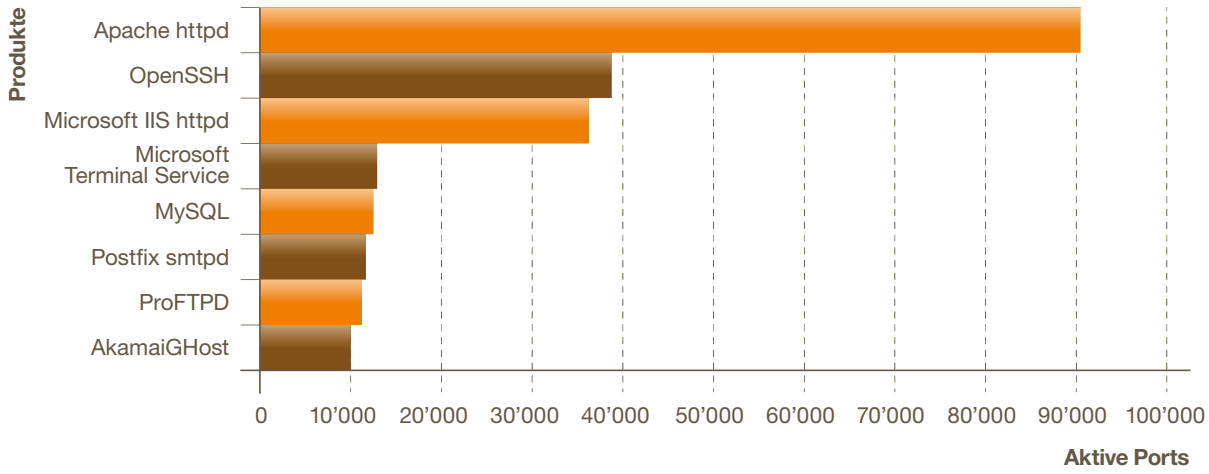
7: Häufigkeit der aktiven Ports

Linux ist das meistverwendete Betriebssystem. Deshalb liegt es nahe, dass Apache als Webserver, OpenSSH für den Remote-Zugriff und MySQL als Datenbank am häufigsten zum Einsatz kommt. Apache ist der Webserver, der in Österreich – und weltweit – am häufigsten verwendet und bei den meisten Hostern als Standardwebserver eingesetzt wird. Neben den Standardports 80 und 443 ist er auf den verschiedensten Ports wie 5000, 8080 oder 8443 aktiv.

An zweiter Stelle steht der IIS-Webserver von Microsoft. Für seine Administration wird oftmals Remotedesktop (Terminalserver) verwendet. Interessant ist das Verhältnis von IIS zu Apache, RDP zu SSH und MSSQL zu MySQL. Es zieht sich mit 1 zu 3 durch diese Drei verschiedenen Dienste (Web, Remote und Datenbank) durch.

Ein Drittel der SMTP Services werden von Postfix angeboten, was durchaus einen sehr guten Marktanteil aufzeigt.

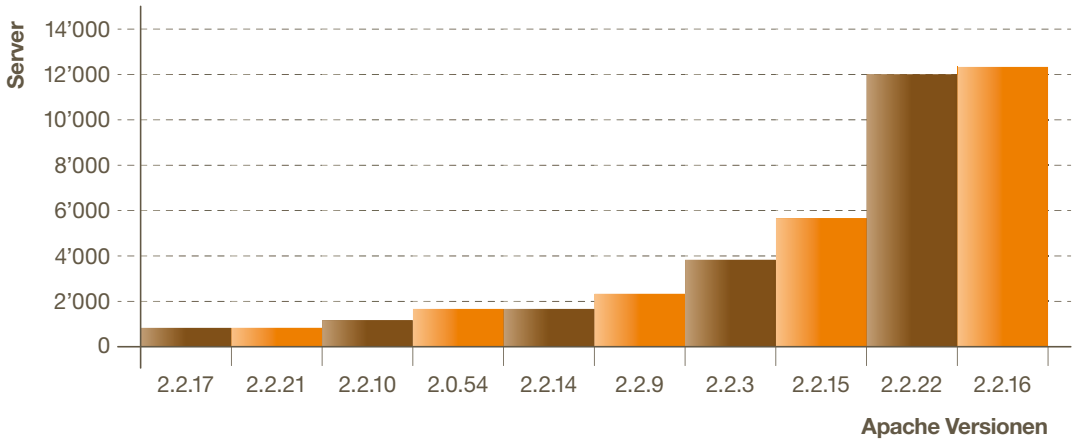
Akamai Global Host ist ein geografisch lokalisierter Caching Server um Webseiten für die Region schneller zur Verfügung zu stellen.



8: Häufigkeit der eingesetzten Produkte

4.3.1 Apache

Von den über 90'000 Apache-Servern gaben über 58'000 ihre Version preis. Am häufigsten werden die 2.2.x-Versionen eingesetzt.



9: Häufigkeit der verschiedenen Apache-Versionen

5. Schwachstellenvorhersage (Vulnerability Forecast)

3,1 Mio
Schwachstellen in Services

7,1 Mio
Schwachstellen in OS

Max CVSS
10.0

Ø Schwachstellen in OS: **40.4**
Ø Schwachstellen in Services: **7.7**

[1] Definition im Glossar

[2] Definition im Glossar

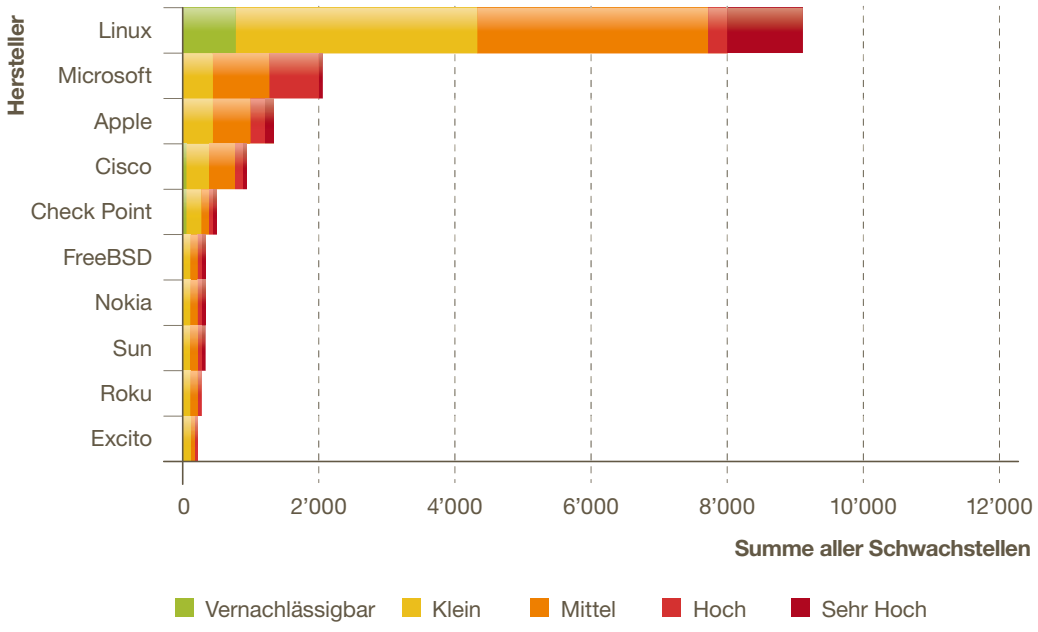
[3] Es handelt sich um potenzielle Schwachstellen und nicht effektive. Patches können Schwachstellen beheben und dabei die Versionen nicht Verändern. Dies führt zu einer gewissen Ungenauigkeit der Resultate. Details unter Punkt 3.2

Sind die Betriebssysteme, Dienste und ihre Versionen identifiziert, lassen sich durch einen Vergleich mit der CVE-Datenbank[1] die potenziellen Schwachstellen ermitteln. Eine solche Vorhersage zeigt mögliche Schwachstellen auf. Diese müssen nicht zwingend tatsächlich vorhanden sein und sich ausnutzen lassen. Über die effektive Bedrohung gäben erst Security Scans Auskunft; solche wurden jedoch, wie in der Einleitung bereits erläutert, für diesen Bericht aus rechtlichen Gründen nicht durchgeführt.

Mit der Schwachstellenvorhersage decken wir ein Potenzial von über 10.2 Millionen Schwachstellen auf. Übertragen auf die eindeutig identifizierten Systeme bedeutet dies: Im Durchschnitt gibt es im Österreichischen Internet 40 OS-Schwachstellen pro eindeutig erkanntes System und knapp 8 pro aktiven Dienst. Die Bedeutung der Schwachstellen kann von klein bis hin zu kritisch reichen. Kritische Schwachstellen entsprechen dem CVSS-Wert[2] von 10. Dies ist der maximal mögliche und bei unseren Untersuchungen auch entdeckte Wert.

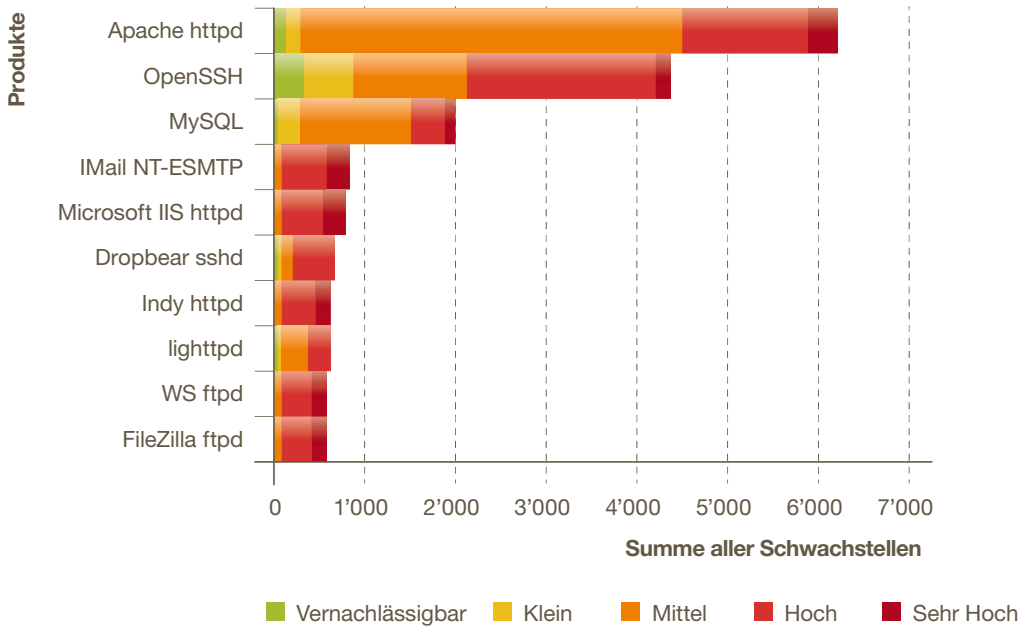
Unsere Inventarisierung ermittelte über 7'500 verschiedene Produkte, die über IP-Adressen ansprechbar sind. Diese verglichen wir mit der CVE-Datenbank, die über 61'000 Schwachstellen kennt.

Abbildung 10 zeigt die Top-10-Betriebssystemhersteller mit den meisten Schwachstellen. Der Schweregrad der Schwachstellen ist in fünf Kategorien unterteilt: vernachlässigbar, klein, mittel, hoch und sehr hoch.



10[3]: Die zehn Hersteller mit den meisten Schwachstellen und ihr Schweregrad

Abbildung 11 zeigt die zehn Produkte mit den meisten Schwachstellen. Der Schweregrad der Schwachstellen ist in fünf Kategorien unterteilt: vernachlässigbar, klein, mittel, hoch und sehr hoch.

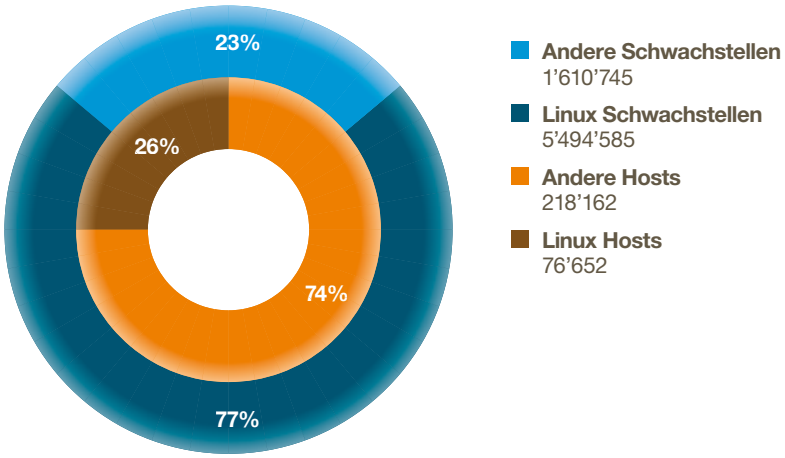


11 [1]: Die zehn Produkte mit den meisten Schwachstellen

5.1 Angreifbare Betriebssysteme

Abbildung 12 visualisiert das Verhältnis von Linux Systemen zu allen anderen Betriebssystemen und die potenziellen Schwachstellen dieser beiden Gruppen.

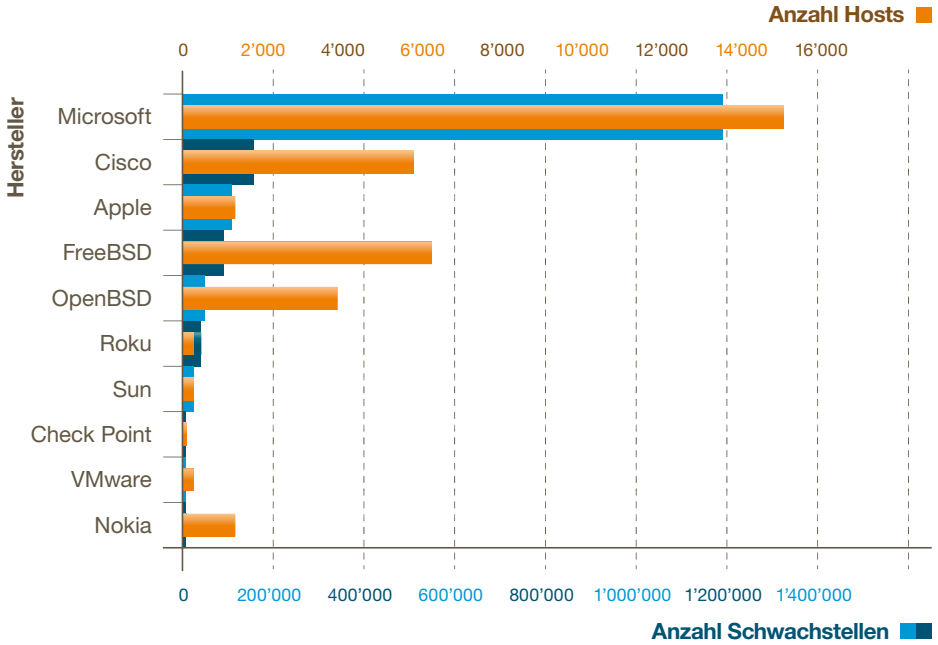
Rund Einviertel der Systeme sind Verantwortlich für Dreiviertel der Schwachstellen.



12 [2]: Linux-Systeme und ihr Anteil an allen Schwachstellen

[1-2] Es handelt sich um potenzielle Schwachstellen und nicht effektive. Patches können Schwachstellen beheben und dabei die Versionen nicht Verändern. Dies führt zu einer gewissen Ungenauigkeit der Resultate. Details unter Punkt 3.2

Die Aufteilung der 23% potenzieller Schwachstellen anderer Betriebssysteme veranschaulicht die Abbildung 13. Apple zählt im Verhältnis zu FreeBSD Fünf mal weniger Systeme und bietet mehr potenzielle Schwachstellen an.

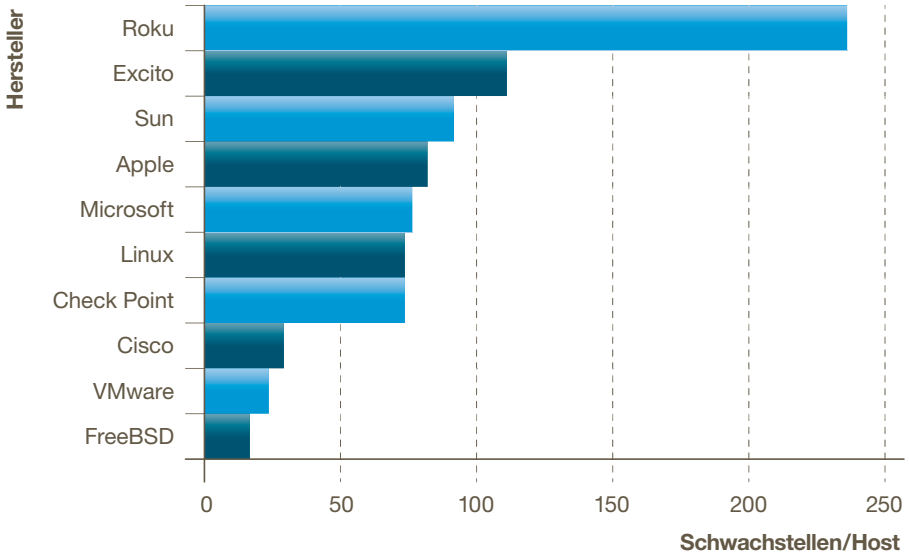


[1-2] Es handelt sich um potenzielle Schwachstellen und nicht effektive. Patches können Schwachstellen beheben und dabei die Versionen nicht Verändern. Dies führt zu einer gewissen Ungenauigkeit der Resultate. Details unter Punkt 3.2

13 [1]: Anzahl Schwachstellen und Anzahl aktive Hosts nach Hersteller ohne Linux

Abbildung 14 zeigt die durchschnittlichen Betriebssystem-Schwachstellen pro Hersteller. Nun tauchen Hersteller wie Roku und Excito mit wenigen aktiven Systemen auf. Beide sind im Entertainment (Home Multimedia Server) tätig und sind für Privatanwender entwickelt worden.

Home Mutlimedialösungen basieren meist auf veralteter Software und bieten oft keine Sicherheitsupdates an.

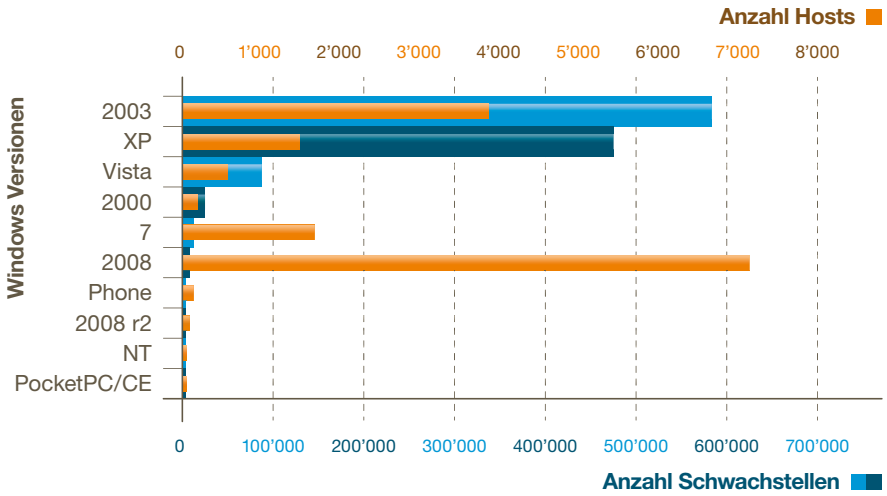


14 [2]: Durchschnittliche Anzahl Schwachstellen pro Host nach Hersteller

5.1.1 Microsoft

Windows 2003 bietet ein grosses Angriffspotenzial mit über 580'000 potenziellen Schwachstellen.

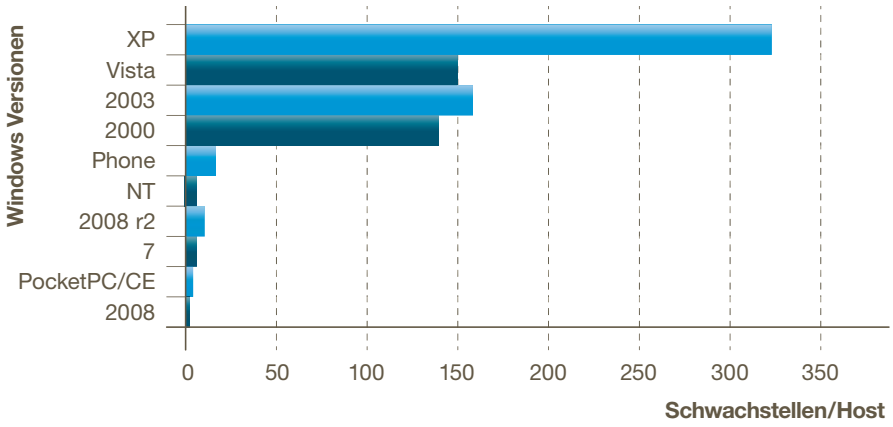
Gefolgt von Windows XP mit knapp 480'000. Die Ablösung von Windows XP und Vista durch Windows 8 und von Windows 2000 und 2003 durch Windows 2012 wird dazu führen, dass sich die Situation der Schwachstellen entschärft. Dies bedeutet aber, dass 6'000 Systeme umzurüsten sind.



15 [1]: Anzahl Schwachstellen und Anzahl aktive Hosts von Microsoft OS

[1-2] Es handelt sich um potenzielle Schwachstellen und nicht effektive. Patches können Schwachstellen beheben und dabei die Versionen nicht Verändern. Dies führt zu einer gewissen Ungenauigkeit der Resultate. Details unter Punkt 3.2

Durch Hersteller nicht mehr unterstütze Betriebssysteme führen zu einer Erhöhung der Schwachstellen und Anfälligkeit dieser Systeme. Abbildung 16 veranschaulicht sehr gut, dass diese Systeme im Durchschnitt am anfälligsten sind. Über die Zeit werden weitere Schwachstellen hinzukommen. Wenn diese Systeme nicht durch aktuelle ersetzt werden, nimmt die Anzahl Schwachstellen in Zukunft massiv zu. Wir rechnen mit ca. 20% mehr Schwachstellen pro Jahr.

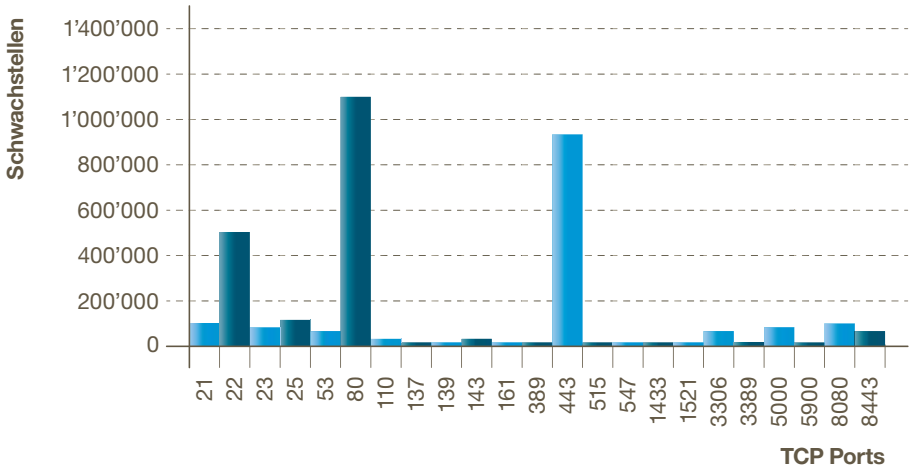


16 [2]: Durchschnittliche Schwachstellen pro aktive Hosts nach Microsoft-OS-Versionen

5.2 Ports mit Schwachstellen

Die Zusammenfassung der Schwachstellen für die einzelnen Ports zeigt eindeutig, dass das grösste Potenzial bei den Webdiensten liegt. Diese machen knapp 70% der potenziellen Schwachstellen aller Services aus. Natürlich können auch andere Services auf diesen Ports betrieben werden. Unsere Analyse ergab, dass bei über 99,9% der beiden TCP Ports 80 und 443 das http-Protokoll eingesetzt wird.

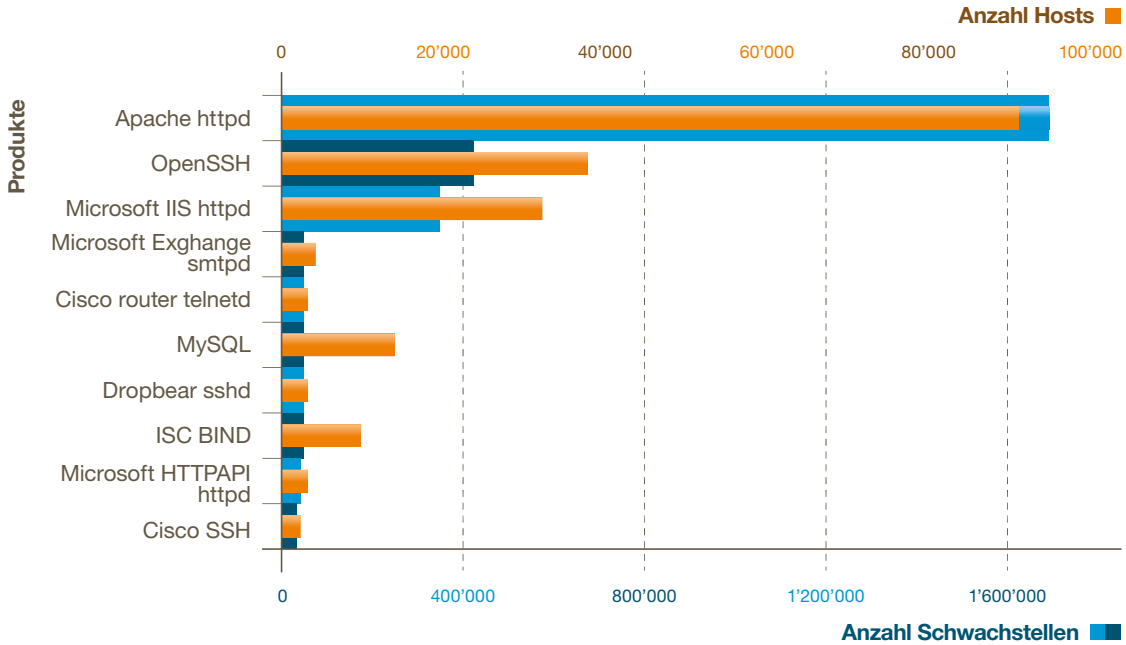
70% der Schwachstellen von Produkten befinden sich in http-Servern.



17 [1]: Anzahl Schwachstellen auf den einzelnen Ports

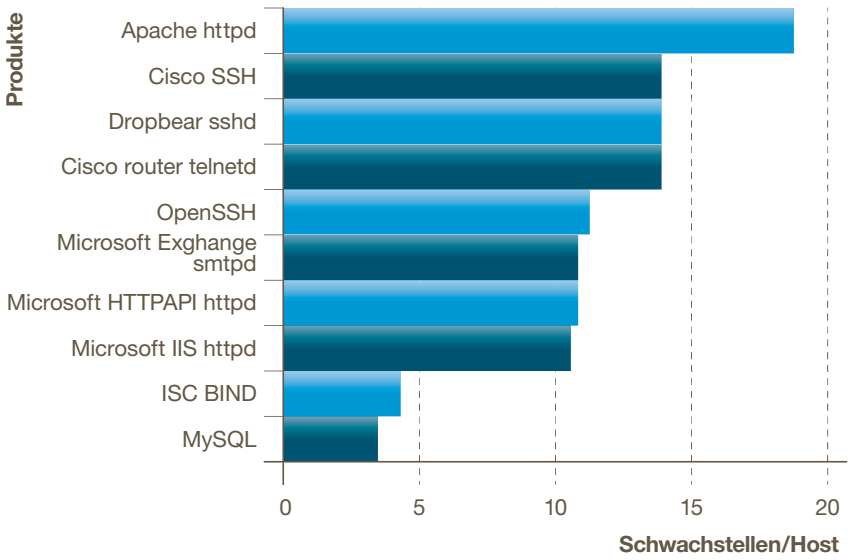
[1-2] Es handelt sich um potenzielle Schwachstellen und nicht effektive. Patches können Schwachstellen beheben und dabei die Versionen nicht Verändern. Dies führt zu einer gewissen Ungenauigkeit der Resultate. Details unter Punkt 3.2

Apache macht mit 1,7 Millionen 79% aller Schwachstellen des http-Protokolls aus. Es fällt auf, dass bei der Abbildung 18 die vier Protokolle http, ssh, smtp und telnet das grösste Angriffspotenzial aufweist.



18 [2]: Anzahl Schwachstellen nach Produkt

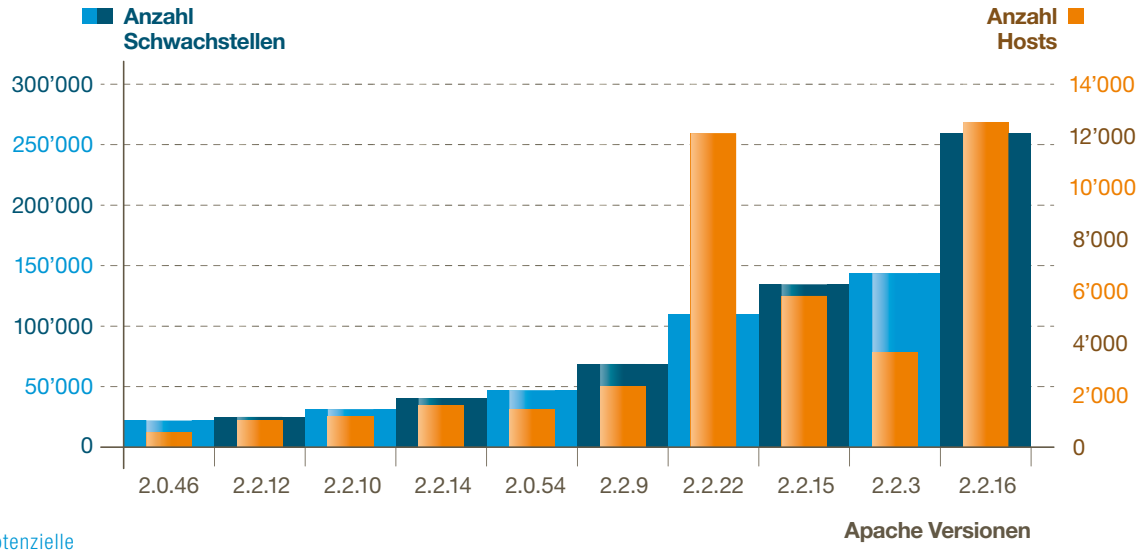
Bei den durchschnittlichen Schwachstellen pro Host führt wenig überraschend Apache. Nachdenklich stimmen die SSH und Telnet Schwachstellen bei Cisco-Routern. Rund 5'200 Routern mit aktiver Telnet- oder SSH-Verbindung fehlen die Updates, respektive sind nicht auf dem aktuellsten Stand. Das Gleiche stellt man bei Dropbear fest. Die über 2'800 identifizierten Dropbear-ssh-Daemons, welche Hauptsächliche in embedded Systemen zum Einsatz kommen, weisen potenzielle Schwachstellen auf. Auch bei Microsoft HTTPAPI, welches für die Kommunikation über http ohne IIS verwendet wird, weisen alle 2'900 gefundenen Dienste potenzielle Schwachstellen auf.



19 [1]: Durchschnittliche Anzahl Schwachstellen pro Host bezogen auf das Produkt

5.2.1 Apache

Die Auflistung der potenziellen Schwachstellen zu den einzelnen Apache Versionen veranschaulicht, dass die Version 2.2.22 über 12'000 Mal zum Einsatz gelangt und im Verhältnis wenig Schwachstellen zu den anderen 2.2.x Versionen aufweist.



[1-2] Es handelt sich um potenzielle Schwachstellen und nicht effektive. Patches können Schwachstellen beheben und dabei die Versionen nicht Verändern. Dies führt zu einer gewissen Ungenauigkeit der Resultate. Details unter Punkt 3.2

20 [2]: Schwachstellen von Apache nach Versionen

6. Fazit

IT-Sicherheit definiert sich über Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und Systeme. Schwachstellen tangieren diese Werte; werden sie ausgenutzt, führt dies dazu, dass Informationen abfliessen, beschädigt oder verweigert werden. In den allermeisten Fällen nutzen die Täter oder Schadsoftware bekannte IT-Schwachstellen aus. Folgende Punkte zeigen einige Möglichkeiten auf, wie sich die IT-Infrastruktur verbessern und die IT-Sicherheit erhöhen lassen.

6.1 Software-Updates

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

6.3 Firewall richtig konfigurieren

Eine Firewall verringert die Angriffsfläche massgeblich. Nicht benötigte Dienste sollten gar nicht erst vom Internet ansprechbar sein. Wir stellen jedoch 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 für ihre Kunden sehr einfach und in kurzer Zeit durch.

6.3 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.

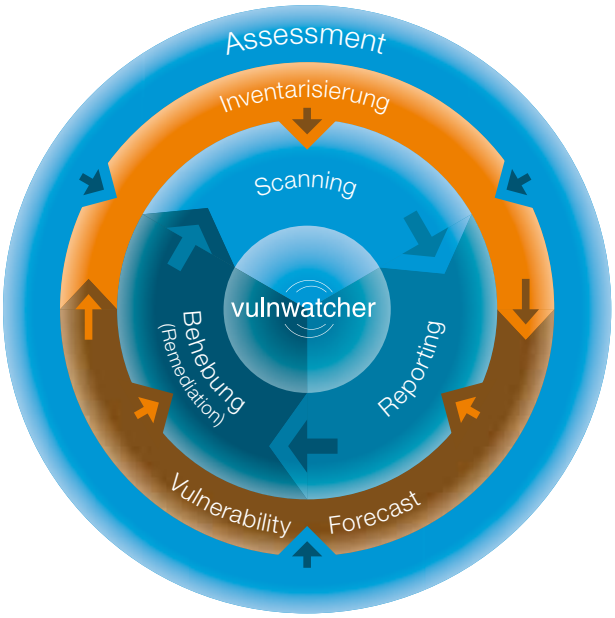
6.4 Benutzerrechte und Passwörter

Viele Benutzer verfügen über Administratoren oder privilegierte Rechte, welche ein erhöhtes Risiko für alle Beteiligten darstellt. Einschränken der Benutzerrechte auf das Notwendigste schützt vor Missbrauch.

Einfache Passwörter finden immer noch sehr häufig Verwendung. Passwortrichtlinien in Bezug auf Komplexität und zeitliche Gültigkeit, one time Password oder 2-Faktor-Authentifizierung erhöhen die Sicherheit.

6.5 Regelmässige Vulnerability Scans

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 durchgeführt haben. So können die aktiven Systeme identifiziert werden. Als Ergebnis erhalten Sie eine Schwachstellenvorhersage. Die tiefe Sicherheitsuntersuchung wiederum deckt 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 vermindern Sie Ihre IT-Risiken und sparen mittel- und langfristig viel Geld.



21: Vulnerability-Management-Prozess

6.6 Security Monitoring

Die Überwachung der wichtigen Systeme auf Verfügbarkeit hat schon länger Einzug gehalten. Wenn ein Dienst nicht läuft, dann wird dies von den Benutzern, Mitarbeiter und Kunden, sehr schnell festgestellt und meist gemeldet. Wie sieht es aber mit der Überwachung von Ereignisse der Systeme und Dienste aus? Eine zentrale Auswertung dieser Informationen hilft Zusammenhänge und Probleme frühzeitig zu erkennen und zu verhindern. Kombiniert mit den Daten aus dem Vulnerability Management erhält man wichtige Daten, Schlüsselwerte, für das Management und IT Dashboard. IT Security wird Messbar.

7. Glossary

7.1 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.

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

7.2 CVE Datenbank

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.

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

7.3 Betriebssystem

Das Betriebssystem ist die Schnittstelle zwischen dem Computer und dem Anwender.

7.4 Schwachstelle

Eine Schwachstelle ist eine Sicherheitslücke in einer Software Applikation.

7.5 Vulnerability

Siehe Schwachstelle.

7.6 Port

Auf einem Port können Verbindungen hergestellt werden, er ist sozusagen die Tür zum Server. Während dem Austrian Vulnerability Scan wurden folgende Ports geprüft:

(Liste mit am meisten verwendeten Dienste)

Port	Protokoll	Name
21	TCP	FTP
22	TCP	SSH
23	TCP	TELNET
25	TCP	SMTP
50	TCP	IKE (VPN)
51	TCP	IMP
53	TCP	DNS
80	TCP	HTTP
110	TCP	POP3
137	TCP	NETBIOS
139	TCP	NETBIOS
143	TCP	IMAP
161	TCP	SNMP
389	TCP	LDAP
443	TCP	HTTPS
515	TCP	LPD
547	TCP	DHCP
1433	TCP	MSSQL
1521	TCP	ORACLE DB
1701	TCP	L2TP
1723	TCP	PPTP
2082	TCP	CPANEL
3306	TCP	MYSQL
3389	TCP	RDP
5000	TCP	UPNP
5900	TCP	VNC/ARD
8080	TCP	HTTP ADMIN
8443	TCP	HTTPS ADMIN

7.7 Österreichisches Internet

In diesem Report sprechen wir vom Österreichischen Internet und verstehen dabei die öffentlichen IP-Adressen, die mit einer Österreichischen 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.

8. 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 2014 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

First Security Technology AG
Bahnhofstrasse 7
CH-7000 Chur

www.first-security.com