Schwachstellen: Gefährlicher Backdoor-Poker

von Peter Tischer am 26.05.2017

Im Zuge der »Wannacry«-Attacke müssen sich Geheimdienste wie die NSA eine Mitschuld an entstandenen Schäden geben lassen. Doch das Zurückhalten von Sicherheitslücken durch Behörden entbindet Unternehmen nicht von einem ausgefeilten Schwachstellenmanagement.

Vor zwei Wochen sorgte die Ransomware »Wannacry« in über 150 Ländern für Chaos auf geschätzt 220.000 Rechnern. In Deutschland war beispielsweise die Deutsche Bahn ein prominentes Opfer, bundesweit fielen Anzeigetafeln und Fahrkartenautomaten aus. Zwar wurde ein integrierter »Kill-Switch« schnell entdeckt und der angerichtete Schaden eingegrenzt, allerdings nutzten die Angreifer eine Lücke im Windows-Betriebssystem, die der NSA schon lange bekannt ist und für die Spähangriffe der Sicherheitsbehörde ausgenutzt wird. Die Kritik von Microsoft an dieser Zurückhaltung seitens der Regierung fiel ungewohnt deutlich aus: Verglichen mit konventionellen Waffen wäre es etwa so, als hätte sich das US-Militär ein paar Tomahawk-Raketen stehlen lassen, echauffierte sich etwa Brad Smith, Chief Legal Officer bei Microsoft. Regierungen müssten einen neuen Ansatz finden, wie sie im Cyberspace dieselben Regeln durchsetzen wie für Waffen in der physischen Welt. Der Windows-Manager ist mit seiner Einschätzung nicht alleine. »Ich begrüße es, dass Microsoft die NSA für die Zurückhaltung von Sicherheitslücken öffentlich angeklagt hat. Denn was uns das eingebracht hat, ist eine Katastrophe«, erklärt etwa Jeremiah Grossman, Chief of Security beim Sicherheitsspezialisten Sentinel One.

Weitere Attacken wie Wannacry sicher

»Wenn wir den Angriff überstanden haben und die Hintergründe genauer beleuchtet wurden, müssen sich die betroffenen Länder und Interessensvertreter zusammensetzen und über Richtlinien und Strategien beraten. Denn es werden weitere Exploits zum Vorschein kommen, die gefährlichen Attacken wie Wannacry die Türe aufhalten«, so Grossman.

Tatsächlich müssen sich Geheimdienste wie die NSA die Frage gefallen lassen, inwieweit dieser gefährliche Backdoor-Poker mit ihrer eigentlichen Aufgabe, den Staat und seine Bevölkerung zu schützen, vereinbar ist. Denn schon jetzt ist absehbar, dass Ransomware-Attacken zur »neuen Normalität« gehören, wie es Grossman ausdrückt. Gelingt es Angreifern, durch nicht gepatchte Sicherheitslücken komplette Infrastrukturen lahmzulegen, stellt das eine direkte Bedrohung von Staat, Gesellschaft und Wirtschaft dar. Die NSA trägt dann in solchen Fällen eine Mitverantwortung.

Doch auch Unternehmen, und hier insbesondere CFOs, sollten ihre Sicherheitsstrategie massiv überdenken. Wenn aus Sparzwang Betriebssysteme wie XP genutzt werden, für die schon seit Monaten keine Sicherheitslücken mehr geschlossen werden, handeln Verantwortliche mindestens genauso fahrlässig wie die kritisierten Geheimdienste. Budgets müssen neu ausgerichtet werden. Zugleich sollten IT-Dienstleister bei etwaigen Problemfällen den Druck auf ihre Kunden erhöhen, in Sachen Sicherheit aufzurüsten. Die Branche bietet inzwischen hoch entwickelte Lösungen an, um die oft manuelle Herangehensweise an das Schwachstellenmanagement zu automatisieren. Ein Invest, der sich angesichts der Bedrohungslage schneller auszahlen dürfte, denn bei Nachlässigkeiten winken mit Inkrafttreten der neuen Datenschutzgrundverordnung zusätzlich saftige Strafen.

»Empfehlungen wie diese sind gewiss nichts Neues – immerhin predigt die IT-Security-Industrie sie seit Jahren –, doch Finanzchefs sind offensichtlich oft nur schwer von Veränderungen zu überzeugen. Es scheint, dass es Weckrufe wie den Wannacry-Angriff braucht, dass erst Menschenleben in Gefahr sein müssen, ehe gehandelt wird«, sagt Grossman.

Kommentar:

Antwort von Peter Langschmidt am 29.05.2017, 14:43 Uhr

mit Interesse habe ich Ihren Artikel über die von Wannacry verwendete Lücke und die Implikationen gelesen.

Aus meiner Sicht haben Sie allerdings eine wesentliche Implikation nicht erwähnt:

Wenn Infrastrukturkomponenten (wie Anzeigetafeln, Krankenhaussysteme etc.) mit einer geplanten Nutzungsdauer von Jahrzehnten mit Software ausgeliefert werden, die nicht mal für ein Jahrzehnt gewartet wird, ist die Katastrophe vorprogrammiert.

Da hier in vielen Fällen weder die Hardware noch die spezifische Software ein Upgrade unterstützen, müsste mit dem Mittel der Produkthaftung gegen die 'Hersteller' vorgegangen werden.

(Wie bekommt man ein 16 Bit Programm auf Windows 10 zum Laufen und wie soll Windows 10 halbwegs performant auf einer Hardware von vor 10 + x Jahren laufen?)

Solange für den geplanten Zweck und Verwendungszeitraum offensichtlich untaugliche Kombinationen von Hard- und Software ungestraft verkauft werden können, sind Wiederholungen der jüngsten Ereignisse auch ohne von Geheimdiensten zurückgehaltene Zero-Day Exploits unausweichlich.

Quelle: http://www.crn.de/security/artikel-113763.html

«Microsoft Office» ist die am stärksten verbreitete Bürosoftware. ...

… und die Gefährlichste. Europa im Würgegriff?

So schlimm ist die Abhängigkeit von Microsoft

Statt auf Open-Source-Software setzen Verwaltungen auf den Quasi-Monopolisten Microsoft. Die wirtschaftlichen Folgen haben unabhängige Journalisten untersucht.

Daniel Schurter **vom 12.04.2017, aktuallisiert am 27.04.17**

Das Wichtigste in Kürze

- In ganz Europa basieren die allermeisten staatlichen IT-Systeme auf Software von Microsoft.
- Weil die IT weiter wächst und immer wichtiger wird, geraten die Staaten immer tiefer in die Abhängigkeit des US-Konzerns.
- Wenn Kunden durch wirtschaftliche Zwänge an einen bestimmten Anbieter gebunden sind, wird dies im Fachjargon **«Lock-in»** genannt.
- Neun europäische Journalisten, die das Recherche-Netzwerk Investigate Europe bilden, haben die Auswirkungen des **Microsoft-Lock-in** während drei Monaten untersucht.
- Befragt wurden Ökonomen, IT-Manager, Sicherheitsexperten und Politiker aus 12 europäischen Ländern sowie die EU-Kommission und Vertreter des Europaparlaments.
- Fazit: Die Software-Abhängigkeit von Microsoft bringt gravierende Nachteile mit sich – für die staatlichen Stellen, aber auch für jeden einzelnen Bürger und jede Bürgerin.
- Die Reaktion von Microsoft folgt weiter unten.

Erschreckende Resultate

Die Ergebnisse seien in verschiedener Hinsicht beunruhigend, fasste der deutsche «Tagesspiegel» in einem am Montag publizierten, ausführlichen Bericht mit dem Titel Europas fatale Abhängigkeit von Microsoft zusammen:

1. Die Abhängigkeit der Staaten von Microsoft **verursache stetig steigende Kosten.** Jahr für Jahr kassiere das Unternehmen allein für die Verteilung von Programm-Kopien an die 50 Milliarden Dollar an Lizenzgebühren.
2. Die Abhängigkeit **blockiere den technischen Fortschritt** in den staatlichen Behörden.
3. Die Abhängigkeit **untergrabe systematisch das europäische Beschaffungs- und Wettbewerbsrecht**.
4. Mit der Abhängigkeit einher gehe ein **erdrückender politischer Einfluss** des US-Konzerns in Europa.
5. Microsoft instrumentalisiere Schulen und Universitäten ungehindert für sein Marketing. Dies sei **«das klassische Drogendealer-Modell»**, urteilte ein Experte. Bis die Kunden abhängig seien, kriegten sie den «Stoff» gratis.
6. Die Abhängigkeit von Microsoft setze die staatlichen IT-Systeme samt den Daten ihrer Bürger einem **hohen technischen und politischen Sicherheitsrisiko** aus.

«Viele staatliche Verwaltungen sind so abhängig von diesem einen Anbieter, dass sie nicht mehr die Wahl haben, welche Software sie nutzen wollen.»
So Informatiker und Jurist Martin Schallbruch, der bis 2016 Abteilungsleiter für Informationstechnik und Cybersicherheit im deutschen Bundesinnenministerium war. quelle: tagesspiegel

Ok, schlimm für die EU. Aber was ist mit der Schweiz?

watson hat bei einem Microsoft-kritischen Wissenschaftler nachgefragt: **Matthias Stürmer** leitet an der Universität Bern die Forschungsstelle Digitale Nachhaltigkeit. Der EVP-Politiker amtet als Geschäftsführer der Parlamentarischen Gruppe Digitale Nachhaltigkeit und setzt sich für Open-Source-Softwares ein.

Die Abhängigkeit von Microsoft sei auch in der Schweiz riesengross, konstatiert der Experte und erinnert an ein folgenschweres Gerichtsurteil in Zusammenhang mit der Beschaffung von Microsoft-Software beim Bund: 2011 unterlagen Open-Source-Anbieter vor Bundesgericht mit einer Beschwerde gegen einen 42-Millionen-Deal. Seither habe die Verwaltung «einen Freipass, Microsoft-Produkte einzukaufen, wie es ihr beliebe».

Es geht auch anders

In einigen Wirtschaftssektoren folge die professionelle Software-Entwicklung längst einem nachhaltigen Prinzip, hält der Tagesspiegel fest. Google oder Siemens etwa arbeiteten in erster Linie mit «Open-Source»-Programmen, also mit Softwares, deren Quellcode offengelegt und mit anderen geteilt wird. Jeder Programmierer und jede Firma dürfe die Open-Source-Software verwenden. Gleichzeitig müssten diese Nutzer ihrerseits alle Verbesserungen, die sie vornehmen, öffentlich zugänglich machen. «So können die Unternehmen zwar mit dem Verkauf solcher Softwares kein Geld verdienen. Gleichzeitig aber nutzen sie die Arbeit von Programmierern rund um die Welt, ohne dafür bezahlen zu müssen.» Sprich: Es profitieren alle, nicht nur ein Quasi-Monopolist.

Pikantes Detail: Das Bundesgericht setzt seit jeher bewusst auf Microsoft-Alternativen. Für das oberste Gericht sei wichtig, die Langlebigkeit der Akten zu garantieren, hält Matthias Stürmer fest. Dieses Ziel sei nur durch den offenen Standard **Open Document Format (ODF)** zu erreichen. Zunächst hätten die Juristen StarOffice genutzt, seit einigen Jahren OpenOffice.org.

«Viele sehen Microsoft als Gott-gegeben an, was ja völlig absurd ist.»
Als zynisch bezeichnet der Wissenschaftler die gängige Praxis beim Bund und anderen öffentlichen Stellen – wie etwa den Kantone Graubünden und Solothurn – «offene Ausschreibungen» für Microsoft-Produkte zu machen. Diese so genannten **«In-Brand Wettbewerbe»** seien ein Witz. Denn bei den Lizenz-Verkäufern herrsche logischerweise kaum Wettbewerb, da sie ihre Lizenzen alle beim Hersteller, also Microsoft, einkaufen müssten.

In der EU herrscht die gleiche (fragwürdige) Vergabepraxis

«(...) Das sei etwa so, als wenn der Staat den Kauf von Autos nur unter den Händlern von Volkswagen ausschreibe, spottet der niederländische Jurist Matthieu Paapst, der die Software-Beschaffung der öffentlichen Hand für seine Doktorarbeit an der Universität Groningen untersucht hat. Sein Fazit: ‹Die Praxis, Microsoft-Produkte für die öffentliche Verwaltung ohne offene Ausschreibung zu beschaffen, bricht das geltende EU-Recht.›»
quelle: tagesspiegel

Damit geht's zurück in die Schweiz:

Einzig in der Stadt Bern forme sich Widerstand gegen Microsoft, hält Matthias Stürmer fest. Dort habe der Stadtrat letztes Jahr einen 843'000-Franken-Kredit genehmigt, um das Potenzial von Open-Source-Software (OSS) zu ergründen.

Noch gebe es aber auch in Bern viele Abhängigkeiten zu Microsoft, so dass mehr als fraglich sei, ob die Stadt selbst bei so einem Kredit «aus der Mangel von Microsoft» komme.

Und auf nationaler Ebene?

Er erhoffe sich sehr, dass die neue Open-Source-Strategie der Bundesverwaltung die Situation verbessere, sagt Stürmer. Bis 2018 soll der Bundesrat einen Plan vorlegen, respektive vorgeben, wie sich die Schweizer Behörden mittelfristig von der Abhängigkeit von Microsoft-Produkten lösen können.

Laut Stürmer muss sich dafür zunächst einmal das Bewusstsein einstellen, dass eine derartige Abhängigkeit von einem einzelnen übermächtigen Anbieter überhaupt ein Problem ist – denn das sei noch längst nicht überall der Fall. «Viele sehen Microsoft als Gott-gegeben an, was ja völlig absurd ist.»

Warum sind Microsoft-Programme gefährlicher als Open-Source-Software?

Es sei kein Zufall, dass alle grossen Hackerangriffe auf staatliche europäische Institutionen in den letzten Jahren stets über Sicherheitslücken in Microsoft-Programmen erfolgten, hält der Tagesspiegel fest. Microsoft-Programme seien komplex (im Vergleich mit der Open-Source-Konkurrenz) und verwundbar. Insbesondere die Bürosoftware («Office») und die damit hergestellten Dateien seien das wichtigste Einfallstor für Cyberattacken.

Dazu passen aktuellen Meldungen über eine manipulierte «Word»-Datei, die das Dridex-Botnet verbreitet und Windows-Computer mit einem Banking-Trojaner infiziert.

«Betroffen sind alle gängigen Versionen des Textverarbeitungsprogramms, inklusive der aktuellsten Variante für Windows 10. Der Fehler in Word erlaubt es Angreifern, ausführbaren Code in Word-Dokumenten zu verschicken. Wird die manipulierte Datei geöffnet, wird eine Verbindung zu einem Server hergestellt, der von den Angreifern kontrolliert wird.»
quelle: futurezone.at

Word-Nutzer sollten derzeit besonders misstrauisch sein bei Mails: Textdokumente sollte man nur öffnen, wenn die Quelle absolut vertrauenswürdig ist.

Und man sollte die Office-Software sofort aktualisieren! Microsoft hat am Dienstag einen «Patch» veröffentlicht, um die Sicherheitslücke zu schliessen.

Was sagt Microsoft?

Microsoft wollte keine der vom Recherche-Netzwerk gestellten Fragen beantworten und verweigerte eine Stellungnahme.

… Die Stadt München setzte jahrelang auf Open-Source-Software, und will nun in die Arme «des Monopolisten» Microsoft zurückkehren. Was steckt dahinter? …

Quelle: https://www.watson.ch/Digital/Schweiz/191718980-Europa-im-W%C3%BCrgegriff--So-schlimm-ist-die-Abh%C3%A4ngigkeit-von-Microsoft

(Blackdoor_in_Microsoftprogrammen.odt/pdf)