Schadprogramme – Gefährdungen für Wirtschaft und Gesellschaft

SICHERHEIT IN IT-NETZWERKEN (TEIL 2) Mittlerweile muss jedem klar sein: Die IT-Sicherheit ist für einen »reibungslosen« Ablauf aller betrieblichen Prozesse ein immens wichtiger Faktor. Die Warnungen von Experten sollten dabei von niemandem in den Wind geschlagen werden, weder vom Privat- noch Geschäftsmann.

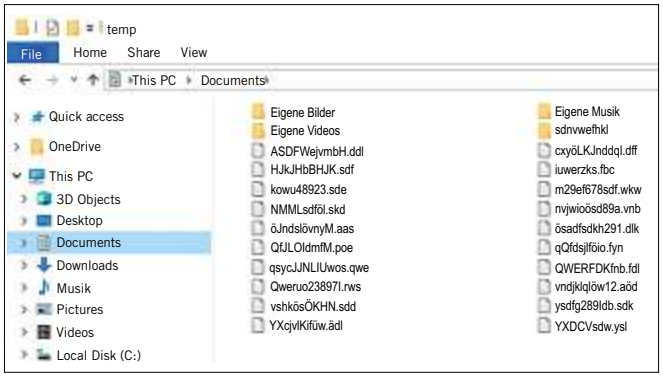
Unternehmen sind selbstverständlich den selben Cyber-Gefahren ausgesetzt wie gewöhnliche Internet-Nutzer. Hinzukommt, dass Unternehmen mit technologischem Fortschritt besonders attraktive Angriffsziele für Cyberkriminelle sind. Ausfälle in der Produktion, im Maschinenpark, Urheberschutzverletzung durch Plagiate oder Erpressung erfordern zudem stärkere Sicherheitsvorkehrungen in der IT-Sicherheit.

Erhebliche Schäden durch Ransomware

Cyber-Angriffe haben erhebliche Konsequenzen für die Wirtschaft, liest man von Seiten des Bundesamts für Sicherheit in der Informationstechnik (BSI). Erpressungstrojaner wie »WannaCry«, »NotPetya« und »Bad Rabbit« brachten 2017 viele Unternehmen weltweit unter Bedrängnis: man spricht hier von Ransomware, ein Schadcode, der innerhalb eines Firmennetzwerks wichtige Ressource wie z.B. Netzlaufwerke, Ordnerstrukturen blockiert, indem er diese verschlüsselt. 2018 setzt sich dies abgeschwächt weiter fort, so das BSI.

Das Bundeskriminalamt (BKA) schreibt in seinem »Bundeslagebild 2017 – Cybercrime«, dass im Sinne einer Bund-Länder-Fallerhebung (2017) von 5191 Malware-Fällen mit 2772 Fällen über die Hälfte durch Ransomware ausgelöst wurden. Die am häufigsten polizeilich angezeigten Ransomware-Familien waren BKA-Trojaner (720 Fälle), »CryptXXX« (170 Fälle), »Cerber« (117 Fälle) und »Locky« (55 Fälle). Neben Unternehmen waren auch Privatpersonen zunehmend davon betroffen.

Ransomware hat die Fähigkeit, sich selbstständig weiter zu verbreiten. Dadurch kommt es immer wieder zu sporadischen, aber begrenzten Infektionen, sobald infizierte, aber nicht auffällig gewordene Rechner Kontakt zu anderen Netzwerken bekommen. Sicher geglaubte interne Netze, die sich auf die Sicherheitsmaßnahmen ihres Umfeldes verlassen, lassen dem Schädling leider nur zu häufig viel Freiraum für eine Weiterverbreitung (**Bild 4**).



Quelle: alle Bilder C. Strobel

Bild 4: Ransomware verschlüsselt Ordner und Dateien

Bild 5: So könnte ein Fenster aussehen, dass Sie bei einem Angriff durch Ransomware zu Gesicht bekommen

Gerade Embedded-Systeme, die für Steuerungen in Industrieanlagen zum Einsatz kommen, sind beliebte Verbreitungswege im industriellen Umfeld. Sie sind oft veraltet und haben nicht gepatchte (nicht ausgebesserte, nicht »geflickte«) Betriebssysteme. Ransomware wie »WannaCry« nutzen dies aus. Manchen Geräten sieht man es nicht unbedingt an, welche Prozesse unter welchem Patchstand und welcher Konfiguration aktuell laufen. Bei »WannaCry« wird das Opfer über den Angriff informiert und erhält eine Lösegeldforderung. Erst mit Zahlungseingang kann das Opfer hoffen, dass die Daten vollständig entschlüsselt werden und der Angreifer von weiteren Forderungen absieht.

Das **Bild 5** wurde einem Dialogfenster des Wanna-Cry-Decryptors nachempfunden. In solchen Fällen sollte das BSI informiert werden (**meldestelle@bsi.bund.de**) Nicht immer ist es aussichtsreich, den Lösegeldforderungen nachzukommen. Die Schadenshöhe von »WannaCry« wurde weltweit bis auf 3,5 Mrd. € beziffert. Diese Summe bezieht sich nicht allein auf den Aufwand der zu zahlenden Lösegelder, die in einer Höhe von nur ca. 100000€ verzeichnet wurden: durch die schnelle Verbreitung des Schadcodes im Unternehmensnetz, müssen betroffene Bereiche identifiziert und gesäubert werden. Die Kosten für die Wiederaufnahme des Betriebs sind deutlich höher als die Lösegeldforderungen. Wer noch mehr über Ransomware, die gegenwärtige Bedrohungslage, Prävention und Reaktion erfahren möchte, kann dies auf der BSI-Seite tun (**Link-Kasten #1**).

Das BKA rät von entsprechenden Zahlungen ab, um das kriminelle Geschäftsmodell Ransomware nicht weiter zu unterstützen. Das Amt schlägt vor, dass sich Ransomware-Opfer durch eine Open-Source-Recherche helfen und die Daten selbst wieder entschlüsseln können (**Bild 6**).

Über zwei Drittel der deutschen Unternehmen sind in den letzten beiden Jahren Opfer von Cyber-Attacken geworden. 50 % der Fälle verliefen erfolgreich für den Angreifer, d.h. es konnten Zugänge zur IT-Infrastruktur erlangt, IT-Systeme beeinflusst oder Webauftritte verändert werden. Produktions- oder Betriebsausfälle folgten ebenfalls bei jedem zweiten Angriff, sowie weitere Folgeschäden durch den Aufwand für die Aufklärung der Vorfälle, das Wiederherstellen des alten Systems oder Imageverlust.

Prozentual verteilen sich die Angriffe wie in **Bild 7** dargestellt. Von den verschiedenen Angriffsarten fanden Malware-Infektionen am häufigsten statt. Sie dringen in IT-Systeme ein und führen schädliche Operationen durch. Beim Hacking erhält ein Eindringling Zugang zu einem Unternehmensnetz. Hacking-Angriffe implizieren Datendiebstahl, Manipulation von Webauftritten oder industriellen Anlagen. DDoS sind verteilte DoS-Angriffe. Sie sind sehr mächtig, weil der Angriff von einem Botnetz, das aus mehreren Rechnern besteht, ausgeht. Sie gefährden die Stabilität von Webservern oder anderen Netzinfrastrukturen.

Wenn der Rechner Teil eines Botnetzes wird

Eine weitere Gefahr für Unternehmen ist das Krypto-Mining. Das BSI sieht diese Angriffsform weiter anwachsen. Beim Krypto-Mining wird im Allgemeinen die Rechenleistung einer IT-Infrastruktur eines Unternehmens dazu verwendet, Bitcoins zu erzeugen. Diese werden später in die Euro-Währung umgetauscht. Bei dieser Angriffsform werden Computersysteme Teil eines Botnetzes. Krypto-Mining-Angriffe sind einfacher feststellbar, da die betroffenen Geräte oft unter Volllast laufen und die Bearbeitungsgeschwindigkeit stark abgebremst wird.

Bisher waren Krypto-Mining-Angriffe nicht effektiv genug. Mit steigender Rechenleistung, vermutet das BSI, ist eine Kehrtwende möglich. Serverinfrastrukturen im Verbund können für das Krypto-Mining interessant werden, auch in Deutschland. Für das Krypto-Mining ist Rechenleistung erforderlich, um »Hashes« (eine Art Prüfsumme) für die »Blockchains« zu berechnen. Eine Blockchain ist eine kontinuierlich erweiterbare Liste von Datensätzen, die dokumentieren, welche Transaktionen auf früheren Transaktionen aufbauen und stellt damit ein dezentrales Buchungssystem dar.

Es gibt spezielle Rechnersysteme, die besonders effektiv Krypto-Mining-Vorgänge verarbeiten. Krypto-Währungen wie Bitcoin, Ripple, Ehtereum oder Tether werden hierdurch gewonnen. Beim Krypto-Mining wirtschaftet der Angreifer auf Kosten der betrieblichen IT-Ressourcen der Opfer.

Im Rahmen der Allianz für Cyber-Sicherheit hat das BSI eine öffentliche Online-Umfrage gestartet. Im Zeitraum vom 4.10. bis 30.11.2017 haben ca. 900 Unternehmen anonym teilgenommen. 58 % der Befragten gaben an, dass Richtlinien wie Notfallpläne oder Störfallanweisungen existieren, damit der Betrieb nach einer schweren Betriebsstörung wiederhergestellt werden kann. Zwei Drittel der großen Unternehmen entwarfen eine solche Richtlinie. Nur die Hälfte der Unternehmen waren kleiner oder mittlerer Größe.

Das BSI empfiehlt den Unternehmen, vorgeplante und aktuelle Notfallpläne zu verwenden. Dies ist eine wichtige Maßnahme und prägt die Qualität der Resilienz (Krisen ohne anhaltende Beeinträchtigungen zu überstehen). Dieser Faktor ist für die Zukunft immer wichtiger, weil es nicht nur darum gehen wird, Opfer eines Angriffs zu sein, sondern diesem auch standzuhalten.

Bild 6: Das Online-Entschlüsselungstool »No more Ransom!« steht unter https://www.nomoreransom.org/ zur Verfügung – es entstand aus der Zusammenarbeit von Europol und einer niederländischen Dienststelle

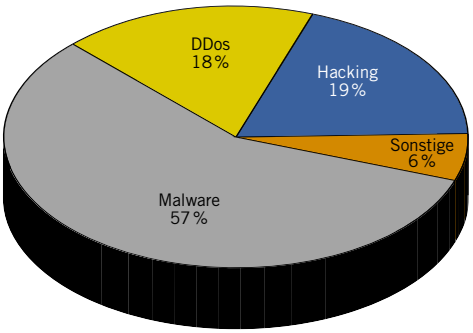


Bild 7: Prozentuale Verteilung der Angriffe auf Firmenrechner im vergangenen Jahr

Gefahren für die Gesellschaft

IT-Lösungen sind ein selbstverständlicher Faktor in vielen gesellschaftlichen Lebensbereichen. Das BSI warnt vor den Gefahren, die sich in den folgenden Bereichen abzeichnen:

- Medizin – smarte Medizintechnik wie z.B. WLAN-fähiger Herzschrittmacher
- Mobile Banking – z.B. fahrlässiges Nutzen von Software und TAN-Generator auf einem Rechner
- Smart Home und IoT (Internet of Things) – z.B. keine Zugangskontrolle bei OBD 2 (OnBoard-Diagnose; Schnittstelle zum Steuergerät)
- Identitätsmissbrauch – z.B. durch Phishing von E-Mail-Adressen, Kennwörtern
- APT (Advanced Persistent Threats) – z.B. Spionagesoftware, Watering Hole-Angriffe
- Gefährdungen von Android-Betriebssystemen und Windows aufgrund deren weiten Verbreitung.

Beim BSI gehen nicht nur Meldungen bezüglich infizierter Systeme ein, es unterstützt Unternehmen in technischer Hinsicht, führt Analysen durch und berät Lösungsansätze. In den Jahren 2017/2018 waren von den gemeldeten Infektionen ca. ein viertel Android- und drei-

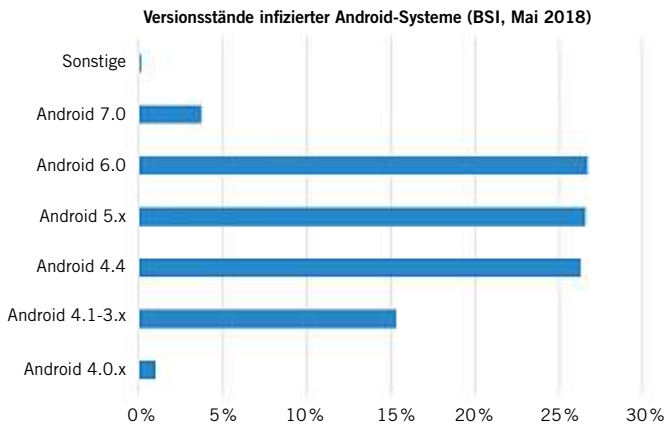


Bild 8: Nur 3,7 % der beim BSI eingegangenen Android-Infektionen betrafen die Version 7.0

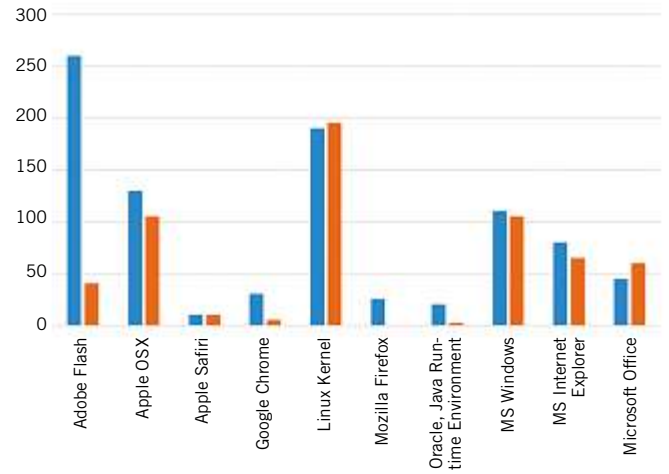


Bild 9: Kritische Entwicklung von Schwachstellen verbreiteter Hard- und Software

viertel Windowssysteme. Eine nachvollziehbare Entwicklung zeichnete sich bei den Android-Systemen ab, wie sie in **Bild 8** aufgezeigt sind.

Die infizierten Geräte konnten durch Botnetze ausgespäht werden – International Mobile Equipment Identity (IMEI)-Nummer oder Standardinformationen ausgelesen und weitergegeben, Schadprogramme nachgeladen oder hochpreisige SMS versandt werden. Wie konnte es dazu kommen? Der Löwenanteil der Android-Infektionen lässt sich auf schadhafte Apps von Drittanbietern zurückführen. Auch veraltete Softwarestände waren dafür verantwortlich. Sie bieten die größere Angriffsfläche – Android 4 hat mit einem Anteil von > 40 % die Nase vorn. Diese Version wird von Google leider nicht mehr unterstützt. Hingegen hat die Version 8 den geringsten Anteil mit ca. 0,2 %.

Welche Gefahren brachte das Jahr 2018 sonst?

Das Institut »AV-Test« führt dafür detailliertere Prüfverfahren zur gezielten Malware-Analyse im großen Umfang durch. Selbstentwickelte Systeme kommen hier zum Einsatz. Die Ergebnisse werden ausgewertet und monatlich veröffentlicht. Das Unternehmen gilt als renommiert. Auch das BSI greift im BSI-Lagebericht 2018 auf die Expertise zurück. Täglich werden mehr als 350000 (!) neue Schadprogramme registriert.

Ein Diagramm auf der Seite **https://www.av-test.org/news/** zeigt den Anstieg von 47,05 Mio. Schadprogrammen im Jahr 2010 bis 856,02 Mio. registrierter Malware Ende 2018. Der Trend setzt sich 2019 fort. Die Ergebnisse vom 8.2.2019 verzeichnen bereits 868,21 Mio. Schadprogramme, einen Zuwachs von weiteren 11,59 Mio. in einem Zeitraum von nur 39 Tagen. Weitere Tests und Statistiken können Sie über die Webseite von AV-Test nachschlagen.

Das BSI überprüft selbst regelmäßig Hard- und Software und bewertet die Gefährdungslage. Auch kombinierte Systeme aus Hard- und Software werden darunter gezählt. Für das Jahr 2018 sind die Bedrohungen unverändert hoch. In den nächsten Jahren wird sich daran nicht viel ändern, so denken Experten. Woran liegt das? Immerhin wird die Hard- und Softwareentwicklung stetig verbessert. Hier einige sicherheitskritische Gegenentwicklungen:

- Endanwendungen werden komplexer
- Software kann aufgrund der modularen Architektur nur teilweise aktualisiert werden
- Software von externen Anbietern (z.B. Treiber) wird nicht geprüft
- Performance und Funktion haben oftmals höhere Priorität gegenüber der Sicherheit und lassen sich besser vertreiben
- Verzicht auf Fehlerbehebung und keine Veröffentlichung von Sicherheitsupdates durch viele Hersteller.

Die Übersicht in **Bild 9** zeigt die kritische Entwicklung von Schwachstellen verbreiteter Hard- und Software: Die Auswertung vergleicht die Anzahl der vom BSI bekanntgewordenen Schwachstellen in den Zeiträumen 1.4.2016 bis 30.3.2017 (blau) und 1.4.2017 bis 30.3.2018 (orange). Es fällt auf, dass der Linux-Kernel überdurchschnittlich viele Schwachstellen gegenüber der Windows-Konkurrenz vorzuweisen hat. Das liegt daran, dass viele Lücken in den Treiber-Modulen gefunden wurden und damit dem Linux-Kernel zugerechnet werden. Bei Windows sind die Treiber externe Software vom Hersteller und werden durch den Endbenutzer eingepflegt. Sie sind nicht Bestandteil des Betriebssystems und werden MS-Windows auch nicht zugerechnet. Der starke Rückgang des Adobe Flash Players lässt sich darauf zurückführen, dass Anfang 2015 mehrfach Sicherheitsmängel festgestellt wurden und der Hersteller nicht direkt mit einem Update darauf reagiert hat. Dadurch war das Vertrauen gebrochen. Viele Browserhersteller deaktivierten das Plugin oder kamen ohne den Multimediaplayer aus. Dadurch ist die Bedrohungslage ebenfalls gesunken. Das BSI informiert auf seiner Seite im IT-Grundschutz-Maßnahmenkatalog M4 (**Link-Kasten #2**).

(Fortsetzung folgt)

LINKS

#1: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Ransomware/Ransomware_node.html

#2: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Massnahmenkataloge/M4HardwareundSoftware/m4hardwareundsoftware_node.html

AUTOR

Claus Strobel
Dozent IT/ET; Schwerpunkt Netzwerktechnik,
Elektro-Technologie-Zentrum, Stuttgart