Viren & Co. – die aktuelle Gefährdungslage

SICHERHEIT IN IT-NETZWERKEN (TEIL 1) Nach Abschluss der Reihe »Richtiger Umgang mit E-Mails« greifen wir das Thema IT-Sicherheit erneut auf und ziehen den Kreis etwas größer: Dabei geht es nicht »nur« um den internen und externen Austausch von Daten, sondern auch speziell um die IT-Infrastruktur (Hardware) und deren Gefährdungen. Beginnen wollen wir mit einer Zusammenfassung zur aktuellen Gefährdungslage in Sachen IT-Sicherheit.

Der Jahreswechsel begann aus Sicht der IT-Sicherheit turbulent. Hier einige Meldungen aus unterschiedlichen Medien der vergangenen Wochen:

- In dem Bericht »IT-Sicherheit: So düster blicken Experten auf 2019« im ZDF am 30.12.2018 (**Link-Kasten #1**) blickt *Falk Garbsch* vom Chaos Computer Club pessimistisch dem neuen Jahr 2019 entgegen; Zitat: »*Es gibt zu viele Baustellen*«.
- Wenige Tage später – am 4.1.2019 – veröffentlichte die Tagesschau »Hackerangriff auf Hunderte Politiker« (**Link-Kasten #2**) einen Riesendatendiebstahl, der von einem einzelnen 20-jährigen Schüler aus Unmut ausgelöst wurde. Persönliche Daten von Promis und Politikern wurden im Internet veröffentlicht.
- Die Süddeutsche Zeitung berichtete dann am 17. Januar 2019 in »Collection #1 – Riesen-Leak von E-Mail-Adressen und Passwörtern aufgetaucht« von einen der größten E-Mail-Account-Angriffen. Ein australischer IT-Sicherheitsexperte hatte die Datensammlung in einem Download-Verzeichnis eines Filesharing-Dienstes zufällig entdeckt. Der Spiegel berichtete von über 772 Mio. gestohlenen E-Mail-Adressen.

Wer wissen möchte, ob seine E-Mail-Adresse ebenfalls in die Hände der Cyber-Kriminellen gelangt ist, kann dies über die BSI-Seite überprüfen (**Link-Kasten #3**).

Wie ist es um die aktuelle Gefährdungslage bestellt? Jährlich veröffentlicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Lage der IT-Sicherheit in Deutschland. Auch das Bundeskriminalamt und AV-Test stellen Ihre Sichtweisen dar. Wir fassen zusammen: Für den Bericht »Lage der IT-Sicherheit in Deutschland« unterteilt das BSI die Bereiche in Bundesverwaltung, kritische Infrastrukturen (KRITIS), Wirtschaft und Gesellschaft innerhalb des Zeitraums 1.7.2017 bis 31.5.2018. Für unsere Zielgruppe sind KRITIS sowie Wirtschaft und Gesellschaft besonders relevant.

LINKS

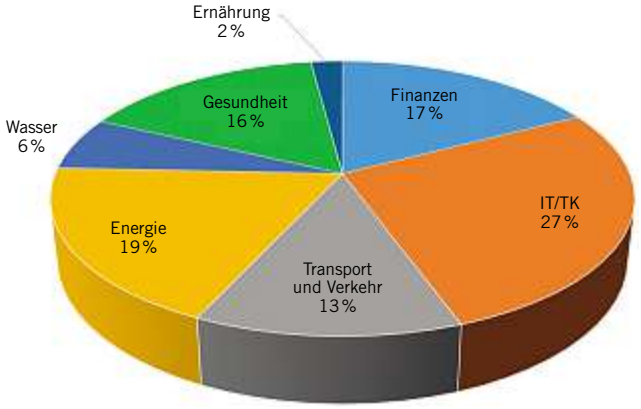
#1: https://www.zdf.de/nachrichten/heute/it-sicherheit-2019-wird-ein-angriffsjahr-100.html

#2: https://www.tagesschau.de/inland/deutsche-politiker-gehackt-101.html

#3: https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/sicherheitstest_02112018.html

#4: https://www.youtube.com/watch?v=qEBLsWwr69Q

#5: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_Uebersicht_node.html



Quelle: alle Bilder C. Strobel

Bild 1: Bereichsmeldungen von »KRITIS« beim BSI in Prozent

Gefährdungen für KRITIS

Kritische Infrastrukturen sind Organisationen und Einrichtungen, die von wichtiger Bedeutung für die Aufrechterhaltung des Gemeinwesens sind. Sie umfassen die Bereiche Gesundheit, Sicherheit, wirtschaftlicher Entwicklung und/oder sozialer Austausch.

Unternehmen der KRITIS versorgen mindestens 500 000 Bundesbürger. Es ist gesetzlich geregelt, welche Sicherheitsvorkehrungen sie einhalten müssen. Sie haben gegenüber der BSI eine Meldepflicht, falls es zu Störungen kommt. Auf Grundlage der Meldungen hat das BSI folgende Beurteilung festgestellt:

- Die Gefährdungslage ist hier außerordentlich hoch. Sie steigt stetig an.
- Der IT-/TK-Bereich ist am stärksten betroffen, danach folgt der Energiesektor.
- Die Angriffsformen sind automatisiert und werden flächendeckend angewendet.
- Gesellschaftliche, politische Ereignisse können die Gefährdungslage weiter schlagartig verändern.

Das **Bild 1** zeigt die prozentuale Verteilung der verschiedenen KRITIS-Bereiche anhand der getätigten Meldungen.

Watering-Hole-Angriffe und Advanced Persistent Threat (APT)

Industrial Control Systeme (ICS) sind besonders vor sogenannten Watering-Hole-Angriffen zu schützen. ICS-Systeme werden als Netz-

werke interpretiert, die Telemetriedaten zu elektromechanischen Komponenten wie Reglern, Ventilen, Verteiler u.a. bereitstellen und steuern. Sie bilden das Rückgrat der Gesamtanlage.

Watering-Hole-Angriffe lassen sich leicht über den Namen ableiten: dazu gehen wir gedanklich nach Afrika, wo es sehr trocken ist. Die Wasserlöcher wirken wie ein Magnet für die Zusammenkunft verschiedener Tiere wie Zebras, Giraffen, Büffel, Flamingos (**Bild 2**). Für den Watering-Hole-Angriff werden Medienereignisse genutzt, um eine große Menge an Personen zu erreichen. Ereignisse wie das Erreichen des Halbfinales der Deutschen Handballnationalmannschaft im Jahr 2019, Hochschneechaos im Süden Deutschlands Anfang des Jahres oder die Hochzeit von Prinz *Harry* und *Meghan Markle* im letzten Jahr können dazu dienen.

Die interessierte Bevölkerung stöbert mit Begeisterung im Internet, um weitere Details zu finden. Auf die Herkunft der Quelle wird nicht immer geachtet. Auf diesem Weg gelangt das Opfer direkt in die Hände des Angreifers. Über eine perfekt nachgemachte Webseite gelangt der Schadcode auf den Büro-Arbeitsplatzrechner des Mitarbeiters. Der Watering-Hole-Angriff war erfolgreich.

Im nächsten Schritt werden Informationen aus der neuen Umgebung gesammelt, wie u.a. Kontaktdaten aus Adressbüchern, Ordner/Netzlaufwerke, Aufbau der IT-Infrastruktur (LAN; WLAN, Bluetooth), Benutzer, Berechtigungen. Er kann veranlassen, dass weiterer Schadcode nachgeladen wird und kann versuchen, so viele »Backdoors« wie möglich zu etablieren. Oft bleibt er an dieser Stelle noch unerkannt und verhält sich wie ein lauerndes Krokodil im Wasserloch (Bild 2).

Selbst für Sicherheitsexperten ist die Bedrohung beim Lesen des Schadcodes nicht erkennbar. Das kann daran liegen, dass der Schädling in einem maschinennahen Programmcode geschrieben ist und nur vom Steuersystem »verstanden« werden kann. Für eine erfolgreiche Schadcodeanalyse sind tiefe ICS-Entwicklerkenntnisse notwendig.

Jetzt ist es nur noch eine Frage der Zeit bis der Schadcode zum ICS-System vorgedrungen ist. Ein ICS-Entwickler hat seinen Entwicklungsrechner auch für Verwaltungstätigkeiten verwendet. Sobald der Schadcode mit dem passenden Steuersystem in Verbindung kommt, kann der Hauptangriff erfolgen. Das Krokodil schnappt zu.

In dieser Phase hat sich in Fachkreisen ein weiterer Ausdruck gebildet, der Advanced Persistent Threat-Angriff (APT). Die Besonderheit liegt darin, dass eine unautorisierte Person innerhalb eines Unternehmensnetzwerks so lange wie möglich unentdeckt bleibt. Informationen sollen gesammelt und Daten ausspioniert werden. Sonstiger Schaden entsteht nicht. Auch wenn APT-Angriffe schwierig zu identifizieren sind, werden Spuren vom Eindringling hinterlassen. Anhand der Analyse des ausgehenden Datenverkehrs lässt sich ein APT-Angriff aufspüren. Vor der weiteren Ausbreitung von APTs warnt der BSI.

Das Beispiel »Stuxnet«

»Stuxnet« (im Jahre 2010) ist ein gutes Beispiel für eine Watering-Hole-Attacke. Rund um den Globus wurden Steuerungscomputer von Industrieanlagen des Herstellers Siemens infiziert. Dabei ging es nicht um die Spionage von Daten, sondern um die Sabotage der Anlage. Trifft Stuxnet auf bestimmte Frequenzregler, wird das Programm aktiv und verändert die Drehgeschwindigkeiten angeschlossener Motoren. Angebundene Vorgänge werden damit gestört. Auf diesem Weg wurde ein gezielter Angriff auf das iranische Atomprogramm in einem unterirdischen, militärisch bewachten Hochsicherheitstrakt in Natanz durchgeführt. Die Zentrifugen zur Urananreicherung fielen in zeitlich

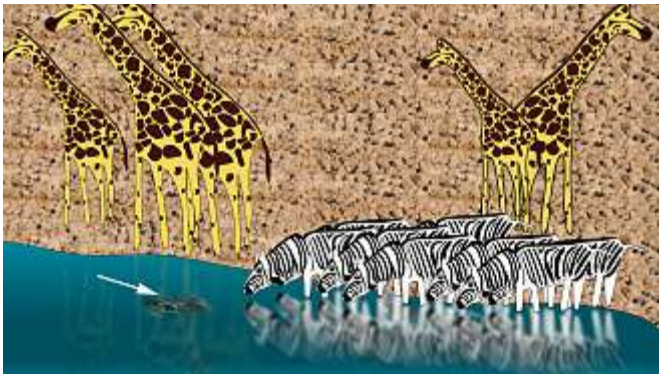


Bild 2: Ein Krokodil lauert im Wasserloch, beobachtet das Geschehen, um plötzlich zuzuschlagen – ein Watering-Hole-Angriff läuft ähnlich ab

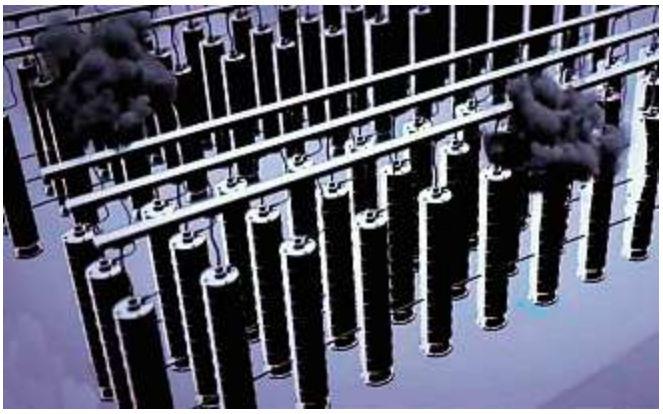


Bild 3: Szene aus dem Film »Cyber-Krieg – wenn das Web zur Waffe wird«

versetzten Abständen nacheinander alle aus. Einen Cyber-Angriff als Ursache fanden iranische Ingenieure anfangs nicht.

Wie konnte der Schadcode auf die Steuerungsgeräte gelangen? Der Schadcode wurde laut dem Sicherheitssoftwarehaus Kaspersky Lab in verschiedenen Länder (auch in Deutschland) nachgewiesen und schädigte verschiedene iranische Industrieanlagen. Stuxnet ist vermutlich mit großer Expertise unter Einbindung verschiedener Spezialbereiche geschrieben worden. Der Schadcode wurde global verbreitet und lief auf verschiedenen Betriebssystemen. Nur bei bestimmten SPS-Systemen wurde er wirksam. Ein Film-Tipp hierzu: Der Nachrichtensender »N24« zeigt in der Dokumentation »Cyber-Krieg – wenn das Web zur Waffe wird« (**Bild 3**) u.a. wie Industrieanlagen durch Cyberkriminelle attackiert wurden (**Link-Kasten #4**).

Wie lassen sich Watering Hole-Angriffe in der Zukunft in den Griff bekommen? Sicherheitsexperten müssen an dieser Stelle mit den ICS-Entwicklern zusammenarbeiten. Das BSI empfiehlt daher, dass sich Unternehmen/Betriebe bereits bei Auffälligkeiten melden, um diese bei der technischen Analyse zu unterstützen. Weitere Informationen hierzu gibt es auf der BSI-Webseite (**Link-Kasten #5**).

(Fortsetzung folgt)

AUTOR

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