Penetrationstests für Stadtwerke

Den Hacker nicht ins Netz lassen

Energieversorgungsunternehmen werden immer häufiger Opfer von Hackerangriffen. Dabei ist oft die nicht genügend gesicherte Schnittstelle zwischen Büro- und Industriesteuerungsnetzwerk die entscheidende Sicherheitslücke, die von Hackern genutzt wird. Durch regelmäßige Penetrationstests können solche Schwachstellen aufgedeckt und entsprechende Gegenmaßnahmen entwickelt werden.

Stanislau, Westukraine: Am 23. Dezember 2015 fällt in rund 700 000 Haushalten für mehrere Stunden der Strom aus. Schon Stunden später wird klar, dass dies nicht durch technische Fehler verursacht wurde, sondern dass Hacker durch gezielte Angriffe auf Energieversorger diese Störung ausgelöst haben. Der slowakische Malware-Spezialist Eset ermittelt und veröffentlicht seine Erkenntnisse in mehreren Blog-Einträgen [1].

Demnach drangen die Hacker bereits Wochen oder Monate vorher per Social Engineering ins Netz des Energieversorgers ein (*Bild 1*). Die Angreifer gaben sich in einer E-Mail als Mitglied des ukrainischen Parlaments aus und verleiteten den Mail-Empfänger auf diese Weise dazu, eine angehängte Excel-Datei zu öffnen. Nach dem »Wegklicken« einer Excel-Warnmeldung folgte unmittelbar die Ausführung der darin enthaltenen Makros und damit die Infektion des PC mit einem Trojaner (*Bild 2*). Dieser trägt den passenden Namen »BlackEnergy Lite« und hat die Aufgabe, weiteren Schadcode aus dem Internet zu laden und das angegriffene System als Sprungbrett in das interne Netz des Energieversorgers zu nutzen.

Die dann folgenden Schritte entsprechen dem klassischen Vorgehen eines Hackers. Das Sprungbrett wird genutzt, um weitere Trojaner-Module nachzuladen und diese zur Infektion vieler Systeme im internen Netz zu verwenden. Zu den infizierten Systemen zählen neben Bürocomputern auch Systeme zur Steuerung der angeschlossenen Industrieanlagen.

Eine der installierten Komponenten heißt »Killdisk« und ist – wie der Name vermuten lässt – dazu geeignet, die Festplatte des infizierten Systems so zu modifizieren, dass sich das System nicht mehr booten lässt. Außerdem kann die Schadsoftware Programme, die zur Steuerung der Industrieanlagen verwendet werden, beenden und so für eine nachhaltige Störung sorgen: Blackout.

Am Ende steht die eher akademische Frage: Wurde der großflächige Stromausfall durch die Infektion selbst verursacht oder war vielmehr die fehlende Reaktionsmöglichkeit auf äußere Einflüsse der wahre Grund für den Ausfall? In jedem Fall zeigt dieses Beispiel, dass erfolgreiche Hackerangriffe auch gegen kritische Infrastrukturen heute schon Realität sind und der Schutz entsprechender Infrastrukturen oberste Priorität haben sollte.

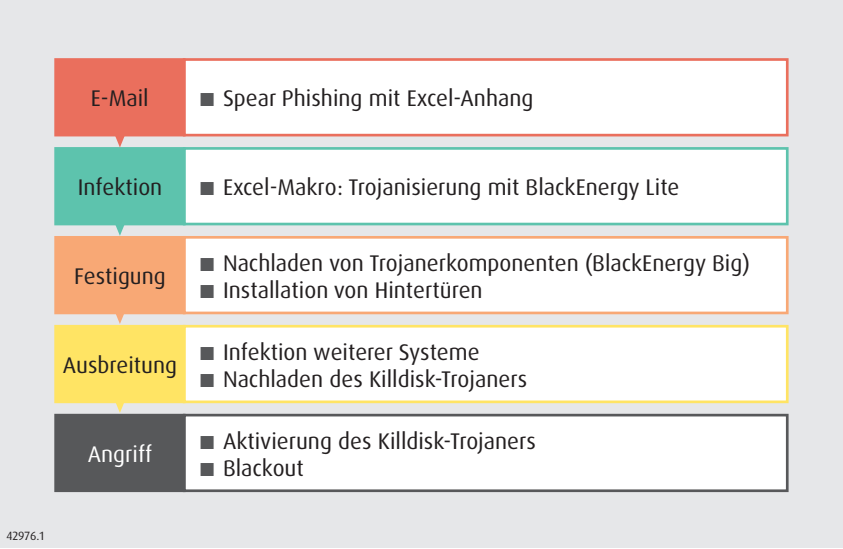

Bild 1. Vorgehensweise bei einem gezielten Hackerangriff auf einen ukrainischen Energieversorger

IT-Sicherheit und kritische Infrastruktur

Der Vorfall in der Ukraine zeigt eindrucksvoll, was die Einleitung zum deutschen IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG in drei Sätzen auf den Punkt bringt: »Unsere moderne Gesellschaft ist in hohem Maß von einer funktionierenden Energieversorgung abhängig. Fehlen Strom und Gas, kommt das öffentliche Leben innerhalb kürzester Zeit zum Erliegen und lebensnotwendige Dienstleistungen können nicht mehr erbracht werden. Gleichzeitig ist das Funktionieren der Energieversorgung von einer intakten Informations- und Kommunikationstechnologie (IKT) abhängig.« Diese Abhängigkeit ist ein Leitgedanke des im Juli 2015 in Kraft getretenen Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und den damit zusammenhängenden Rechtsverordnungen. Den Betreibern kritischer Infrastrukturen, zu denen auch die Energie- und Wasserversorger gehören, wird damit also ein sorgfältiger Umgang mit IT-Sicherheit gesetzlich vorgeschrieben, auch wenn die konkrete rechtliche Ausgestaltung und Umsetzung derzeit noch nicht vollständig abgeschlossen ist.

Umso wichtiger ist es, sich bereits jetzt in den betroffenen Betrieben, zu denen auch Stadtwerke ab einer in der Anfang April 2016 vom Bundeskabinett gebilligten, aber noch nicht in Kraft getretenen BSI-Kritis-Verordnung definierten Größe gehören – zum Beispiel 120 Anlagen zur Stromerzeugung [2] –, Gedanken über konkrete Schritte zur Umsetzung der neuen gesetzlichen Anforderungen zu machen. Eine Maßnahme, die sich seit Jahren branchenübergreifend als verlässliches Prüfverfahren etabliert hat, ist die regelmäßige und systematische Durchführung von Penetrationstests.

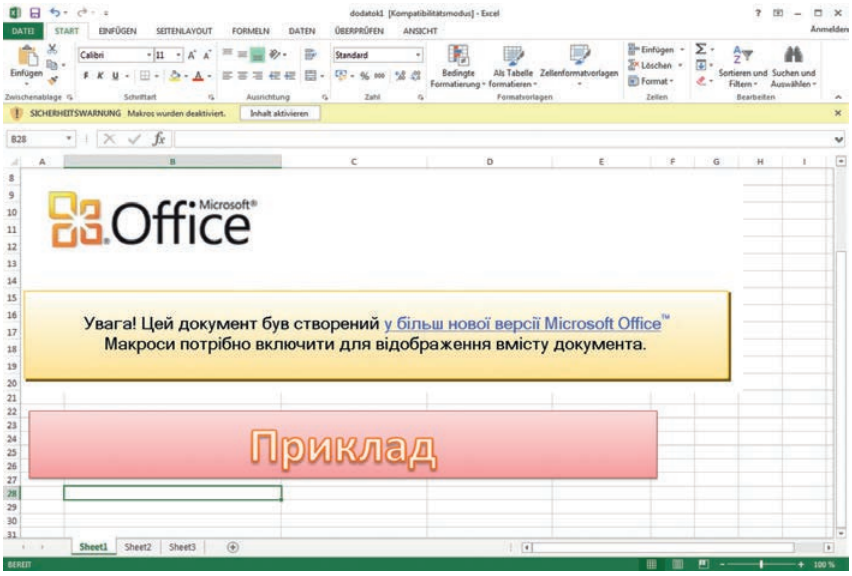

Bild 2. Das zur Trojanisierung verwendete Excel-Dokument

Penetrationstest: Planung, Durchführung, Ziele

Verbreitete Maßnahmen der IT-Qualitätssicherung – zum Beispiel Code-Reviews, Security Development Lifecycle sowie Grundschutz- und ISO-Zertifizierungen – können eventuell ausreichen, um 99 % der IT-Infrastruktur eines Unternehmens zu sichern. Dabei bleibt jedoch ein entscheidendes Problem: Das verbleibende 1 % Verwundbarkeit kann von Angreifern gezielt gefunden werden. Das heißt: Auch eine sehr kleine Lücke genügt, um eine ansonsten gut abgesicherte IT-Infrastruktur angreifbar zu machen. Reale Hacker nutzen ihr Know-how, um genau dieses 1 % Unsicherheit zu erkennen und gezielt anzugreifen.

Auch ein Penetrationstester setzt an dieser Stelle an, jedoch mit anderer Intention: ein Penetrationstest simuliert eine echte Hackerattacke und deckt auf diese Weise vorhandene Sicherheitslücken auf – noch bevor diese missbraucht werden können. Dabei sollte es jedoch nicht bei einer einmaligen Prüfung bleiben: Täglich werden neue Sicherheitslücken in Softwareprodukten gefunden, die den Handlungsspielraum für digitale Angreifer erweitern. Penetrationstests sollten deshalb in feste Prüfpläne integriert sowie entsprechend häufig und in einem festen Rhythmus durchgeführt werden. Der einzelne Test untersucht ein oder mehrere Angriffsszenarien. Der Auftraggeber definiert dabei folgende Spezifika in Hinblick auf das eigene Unternehmen:

1. Angriffsursprung (von wo?)
2. Angriffsziel Scope (was?)
3. Testtiefe (wie lange?)
4. Testmittel (wie?)
5. Wissensstand und Motivation des Angreifers (wer?).

Wer als Penetrationstester erfolgreich sein will, sollte seine IT-Spezialkenntnisse immer auf dem neuesten Stand halten. Doch nicht nur aus diesem Grund empfiehlt es sich, entsprechende Untersuchungen nicht nur mit internem Personal durchzuführen: Eine unternehmenseigene Fachabteilung hat nicht nur ein sehr breites Aufgabenspektrum, sondern unterliegt auf Dauer auch dem Risiko, »betriebsblind« zu werden. Der regelmäßige Blick von außen durch einen unabhängigen Penetrationstester hilft, blinde Flecken aufzudecken und Sicherheitsprobleme zu beheben, bevor es zu einem realen Angriff kommen kann (*Bild 3*).

Energie- und Wasserversorger: »Normale« Unternehmen mit besonderen Anforderungen

Aus Sicht eines Penetrationstesters ist ein Energie- und Wasserversorger im ersten Schritt ein normales Unternehmen. Im obligatorischen Büronetzwerk der Verwaltung und weiterer vergleichbarer Abteilungen sind üblicherweise eine Reihe normaler Desktoprechner oder Notebooks im Einsatz. Dazu kommen Windows- oder Linux-Server zum Beispiel für den Dateiaustausch und den E-Mail-Verkehr. In dieser Hinsicht unterscheiden sich klassische Stadtwerke zunächst nicht von einem ortsansässigen mittelständischen Unternehmen. Das Büronetzwerk dient unter anderem zur Abwicklung alltäglicher Verwaltungsaufgaben und der Bearbeitung und dem Austausch von Dokumenten.

Auf den zweiten Blick unterscheidet sich ein Energieversorger jedoch deutlich vom Standardunternehmen: Neben dem Büronetzwerk gibt es noch eine zweite Infrastruktur – die zur Steuerung von Industrieanlagen. Kraftwerke, Umspannwerke, Photovoltaikanlagen und alle mit diesen Anlagen zusammenhängenden Prozesse werden aus diesem Netzwerk über entsprechende Scada-Systeme (Supervisory Control and Data Acquisition) gesteuert. Über dieses technische Netzwerk kann ein Techniker zum Beispiel eine PV-Anlage vom Netz nehmen, wenn diese bei intensiver Sonneneinstrahlung eine Überlast erzeugt, die sich negativ auf die Netzstabilität auswirken würde. Im Umkehrschluss heißt das aber auch – und hier liegt die große Gefahr: Wenn sich ein Hacker Zugang zu diesem Netz verschafft, können kritische Anlagen manipuliert und so eventuell erhebliche Schäden angerichtet werden. Anstatt an einem heißen Sommertag PV-Anlagen vom Netz zu nehmen, könnte der Hacker vielmehr alle vorhandenen Anlagen zuschalten und so eine Überlastung des Stromnetzes herbeiführen und Stromausfälle verursachen.

Doch wie kommt der Hacker in das Industriesteuerungsnetz? Die Antwort lautet: meist über eine undichte Stelle im Büronetzwerk. Üblicherweise gibt es zwischen beiden Netzen Übergänge, zum Beispiel damit ein Techniker auch von seinem Bürorechner Zugriff auf technische Informationen von laufenden Anlagen hat. Entscheidend für die Sicherheit des Netzes ist die Art und Weise, wie der Übergang vom Büro- ins Steuerungsnetz gestaltet ist. Ist die Netzwerktrennung konsequent und durchgängig realisiert? Sind vorhandene Zugänge über ein solides Virtual Private Network (VPN) abgesichert? Sind Scada-Steuerungen über Webinterfaces via Intranet oder sogar via Internet erreichbar?

Ausgehend von diesen Überlegungen geht auch der Penetrationstester zweistufig vor. Zunächst wird das Büronetzwerk auf mögliche Schwachstellen und Einfallstore für Schadsoftware (Malware) überprüft. Gelingt es dem Tester, zum Beispiel über einen mit Malware infizierten E-Mail-Anhang einen Trojaner auf einen Büroclient zu schleusen, ist der Schritt zu einer Ausbreitung der schädlichen Software im ganzen Büronetzwerk nicht mehr weit. Die im Frühjahr 2016 immer wieder aufgetretenen Fälle in Krankenhäusern und öffentlichen Verwaltungen, in deren Netzwerken sich

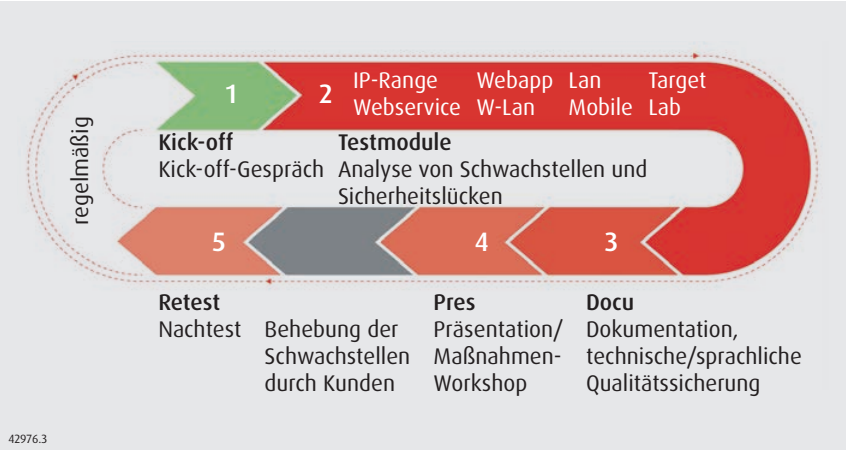

Bild 3. Ablauf eines Penetrationstests

Krypto-Trojaner ausbreiteten, sind nur ein Beispiel dafür, dass dieser Verbreitungsweg noch immer zu den häufigsten zählt.

Hat es der Penetrationstester geschafft, sich mit der eingeschleusten Schadsoftware entsprechende Zugriffsrechte im Büronetzwerk zu verschaffen, macht er sich auf die Suche nach eventuell vorhandenen Schnittstellen zum Industriesteuerungsnetzwerk. Wird er fündig, folgt der zweite Schritt: Wie gut ist der Zugang zum technischen Netzwerk abgesichert? Verwendet der Techniker eventuell dasselbe – schwache – Passwort für seinen Windows-Rechner und den Zugang zur Steuerung der PV-Anlage? Oder sind gar Scada-Websteuerungen vorhanden, die noch das herstellerseitig gesetzte Standardpasswort verwenden? Wird der Tester hier fündig, ist ein heikler Punkt erreicht – und der Auftraggeber wird augenblicklich telefonisch benachrichtigt.

Der Versuch, tatsächlich die Steuerung einer unzureichend abgesicherten Anlage zu manipulieren, gehört nicht zu den Aufgaben des Penetrationstesters. Es soll nur vor Augen geführt werden, welche weitreichenden Schäden ein illegaler Hacker, der sich auf demselben Weg Zugang verschafft, anrichten könnte. Gelingt es dem Penetrationstester im Fall eines Energieversorgers etwa nachzuweisen, dass es möglich ist, ein Umspannwerk von außen über das Internet zu manipulieren, lässt sich an dieser Stelle wohl schwerlich noch ein sachliches Gegenargument finden: Die IT-Sicherheit des Versorgers und die damit verknüpfte Betriebssicherheit der Anlagen sind offensichtlich nicht gewährleistet und es sollten umgehend Gegenmaßnahmen ergriffen werden.

Hierzu liefert ein Penetrationstest bereits einen konstruktiven Beitrag, denn der Abschlussbericht dokumentiert nicht nur alle Sicherheitsschwächen, sondern enthält auch konkrete Vorschläge, um diese zu beseitigen. Dabei sollte jedoch berücksichtigt werden, dass täglich neue Sicherheitslücken entdeckt und im Internet veröffentlicht werden. Deshalb gilt: Je komplexer und je schutzwürdiger die IT-Infrastruktur eines Unternehmens ist, desto häufiger sollten Penetrationstest durchgeführt werden. Für Betreiber kritischer Infrastrukturen sind – nicht nur angesichts der aktuellen Gesetzeslage – regelmäßige Penetrationstests das Mittel der Wahl, wenn es darum geht, die Angriffsfläche für Hacker zu minimieren.

Literatur

[1] Black Energy Trojan Strikes again: Attacks Ukrainian Electric Power Industry. www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry.

[2] Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz. Stand 13. April 2016.

Sebastian Schreiber,
Geschäftsführer,
Syss GmbH, Tübingen

>> sebastian.schreiber@syss.de

>> www.syss.de

42976