Suisse Cyber Security

! ES GIBT KEINE zweite CHANCE, DEN ersten erfolgreichen ICT- / CYBER- ANGRIFF IM UNTERNEHMEN SCHADLOS ZU ÜBERSTEHEN !

KMU verschlafen die Computer- Sicherheit meist komplett – Forensik im Cyber Einsatz

(ein Suisse Cyber Security InHouse- Interview mit ICT- Forensiker und SCSC Jens B. mit Beispielen aus Deutschland und anderen Ländern, welche durchaus auch für die Schweiz sinngemäss ihre Gültigkeit haben)

Nach gesammelten Erkenntnissen sind alle Unternehmen nur unzureichend gegen Cyberangriffe geschützt, mahnt Jens. Die Attacken nehmen deutlich zu, doch viele Unternehmen gehen noch immer zu sorglos mit dem Thema um.

Um zu verdeutlichen, wie gross die Bedrohung ist, und auch zur Veranschaulichung dieser, greift die IT- Sicherheitsbranche inzwischen zu Hollywood- Methoden in der Cyber- Forensik, denn Hacker greifen mittlerweile auch die Filmindustrie an.

Die Branche lebt zwar von der Gefahr durch Hackerangriffe wie Hollywood vom Film- Blockbuster. Die Gefahr ist inzwischen so gross, das man meinen könnte, dass die Digitalisierung sei in Gefahr sei: "Wir sind heute noch alle viel zu naiv bei der Digitalisierung, wenn man bedenkt, dass ca. 380.000 Malware Programme täglich neu hinzukommen", sagt der Cybercrime Experte Jens. Eine Firewall und ein Anti-Virenprogramm reichen bei weitem noch nicht aus. Vielmehr ist die Person hinter dem Bildschirm oft verantwortlich für Datendiebstahl.

Es sind Nachrichten wie diese, die Experten aufhorchen lassen: Hackerangriffe auf deutsche Wasserversorgungsanlagen führen zu Störungen. Erpressersoftware legt die IT des Lukas Krankenhauses in Neuss lahm. Das Gesundheitssystem in Grossbritannien wurde ebenfalls von Hackern lahm gelegt, World- Disney wurde

mit der Vorveröffentlichung des neuesten „Fluch der Karibik 5" erpresst. Wer denkt, dass kann meinem Unternehmen nicht passieren, befindet sich auf einem falschen Weg, will keine Investition in die IT stecken oder sieht die Problematik nicht. Und: Die Erpressersoftware "Locky & Co" machen seit Wochen und Monaten die Haus- IT in Unternehmen nervös, weil sie nicht nur die lokalen Rechner, sondern auch Daten im Netzwerk verschlüsseln.

Die Gefahr ist gross, und sie nimmt parallel zur fortschreitenden Digitalisierung zu: Aufzeichnungen zufolge waren bereits rund die Hälfte der deutschen Unternehmen in den vergangenen zwei Jahren Opfer von Cybercrime. Genaue Zahlen gibt es nicht, denn viele Betroffene melden sich nicht bei den Behörden - vor allem aus Sorge darum, dass sich die Ermittler Zugang zu ihren Daten und Sicherheitssystemen verschaffen müssen, um die Hacker zu schnappen – wobei Unternehmen mittlerweile nach dem BDSG (Bundesdatenschutzgesetz DE) verpflichtet sind, solche Angriffe den Behörden zu melden. Meist sind die Unternehmer ahnungslos, dass sie illegal handeln. Bussgelder von 2% des Jahresumsatzes, bis zu 20 Millionen Euro, können verhängt werden. Aber, laut einer Studie des Branchenverbands Bitkom schaltet nur jedes fünfte betroffene Unternehmen staatliche Stellen ein.

Was zudem viele auch nicht wissen: sie als Unternehmer haben vielleicht Rechner vom Hersteller Apple, auf denen sie Angebote, Rechnungen, Mahnwesen, etc. verwalten. In der Kombination mit dem Cloud- Backup System von Apple verstossen sie bereits gegen das BDSG. Warum? Weil Apple mit Ihnen keine Auftragsdatenverarbeitung (Ihre Daten liegen auf Apple- Server) nach §11 BDSG bestätigen wird.

Das gleiche gilt übrigens auch für Nutzer von Google- Drive.

Erste Anzeichen dass sie gehackt wurden

Software installiert sich selbstständig

Ungewollte und unerwartete Installationsprozesse, die aus dem Nichts starten, sind ein starkes Anzeichen dafür, dass das System gehackt wurde. In den frühen Tagen der Malware waren die meisten Programme einfache Computerviren, die die "seriösen" Anwendungen veränderten - einfach um sich besser verstecken zu können. Heutzutage kommt Malware meist in Form von Trojanern und Würmern daher, die sich wie jede x-beliebige Software mittels einer Installationsroutine auf dem Rechner platziert. Häufig kommen sie "Huckepack" mit sauberen Programmen - also besser immer fleissig Lizenzvereinbarungen lesen, bevor eine Installation gestartet wird. In den meisten dieser Texte, die niemand liest, wird haarklein aufgeführt, welche Programme wie mitkommen.

Suisse Cyber Security

! ES GIBT KEINE zweite CHANCE, DEN ersten erfolgreichen ICT- / CYBER- ANGRIFF IM UNTERNEHMEN SCHADLOS ZU ÜBERSTEHEN !

Die Maus hüpft über den Monitor, ohne dass sie sie benutzen

Hüpft der Mauszeiger wie wild über den Bildschirm und trifft dabei Auswahlen oder vollführt andere Aktionen, für deren Ausführung im Normalfall geklickt werden müsste, ist der Computer definitiv gehackt worden. Mauszeiger bewegen sich durchaus schon einmal von selbst, wenn es Hardware- Probleme gibt. Klick-Aktionen jedoch sind nur mit menschlichem Handeln zu erklären.

Stellen sie sich das so vor: Der Hacker bricht in einen Computer ein und verhält sich erst einmal ruhig. Nachts dann, wenn der Besitzer mutmasslich schläft (der Rechner aber noch eingeschaltet ist), wird er aktiv und beginnt, das System auszuspionieren - dabei nutzt er dann auch den Mauszeiger.

…was nun?

Wenn Ihr Rechner des Nachts von selbst "zum Leben erwacht", nehmen sie sich kurz Zeit, um zu schauen, was die Eindringlinge in Ihrem System treiben. Passen sie nur auf, dass keine wichtigen Daten kopiert oder Überweisungen in Ihrem Namen getätigt werden. Am besten einige Fotos vom Bildschirm machen (mit der Digitalkamera oder dem Smartphone), um das Eindringen zu dokumentieren. Anschliessend können sie den Computer ausschalten - trennen sie die Netzverbindung (wenn vorhanden, Router deaktivieren) und rufen sie die Profis. Denn nun brauchen sie wirklich fremde Hilfe.

Anschliessend nutzen sie einen anderen (sauberen!) Rechner, um alle Login-Informationen und Passwörter zu ändern. Prüfen sie Ihr Bankkonto - investieren sie am besten in einen Dienst, der Ihr Konto in der folgenden Zeit überwacht und sie über alle Transaktionen auf dem Laufenden hält. Um das unterwanderte System zu säubern, bleibt als einzige Möglichkeit die komplette Neuinstallation. Ist Ihnen bereits finanzieller Schaden entstanden, sollten IT- Forensiker vorher eine vollständige Kopie aller Festplatten machen. sie selbst sollten die

Strafverfolgungsbehörden einschalten und Anzeige erstatten. Die Festplattenkopien werden sie benötigen, um den Schaden belegen zu können.

Online- Passwörter ändern sich plötzlich

Wenn eines oder mehrere Ihrer Online- Passwörter sich von einem auf den anderen Moment ändern, ist entweder das gesamte System oder zumindest der betroffene Online- Dienst kompromittiert. Für gewöhnlich hat der Anwender zuvor auf eine authentisch anmutende Phishing- Mail geantwortet, die ihn um die Erneuerung seines Passworts für einen bestimmten Online- Dienst gebeten hat. Dem nachgekommen, wundert sich der Nutzer wenig überraschend, dass sein Passwort nochmals geändert wurde und später, dass in seinem Namen Einkäufe getätigt, beleidigende Postings abgesetzt, Profile gelöscht oder Verträge abgeschlossen werden.

Suisse Cyber Security

! ES GIBT KEINE zweite CHANCE, DEN ersten erfolgreichen ICT- / CYBER- ANGRIFF IM UNTERNEHMEN SCHADLOS ZU ÜBERSTEHEN !

Gefälschte Antivirus- Meldungen

Fake- Warnmeldungen des Virenscanners gehören zu den sichersten Anzeichen dafür, dass das System kompromittiert wurde. Vielen Anwendern ist nicht bewusst, dass in dem Moment, wo eine derartige Meldung aufkommt, das Unheil bereits geschehen ist. Ein Klick auf "Nein" oder "Abbrechen", um den Fake-Virusscan aufzuhalten, genügt natürlich nicht - die Schadsoftware hat sich bestehende Sicherheitslücken bereits zunutze gemacht und ist ins System eingedrungen.

Bleibt die Frage: Warum löst die Malware diese "Viruswarnung" überhaupt aus? Ganz einfach: Der vorgebliche Prüfvorgang, der immer Unmengen an "Viren" auftut, wird als Lockmittel für den Kauf eines Produkts eingesetzt. Wer auf den dargestellten Link klickt, gelangt auf eine professionell anmutende Website, die mit positiven Kundenbewertungen und Empfehlungen zugepflastert ist. Dort werden Kreditkartennummer und andere Rechnungsdaten abgefragt - und immer noch viel zu viele Nutzer fallen auf diese Masche herein und geben ihre Identität freiwillig an die Kriminellen ab, ohne etwas davon zu merken.

Was zu tun ist: Computer ausschalten, sobald die gefälschte Antivirus- Meldung aufschlägt. (Achtung: sie müssen natürlich wissen, wie eine "echte" Meldung Ihres Virenscanners aussieht.) Was nun noch bleibt, ist ein umfassender Systemtest und ein kompletter Virenscan durch Fachleute, um die letzten Reste der Malware zu entfernen.

| JENS B. - SCSC (Senior Cyber Security Consultant) im Suisse Cyber Security InHouse- Interview mit:
| ROGER REINHARD
| CEO & CCSC (Chef Cyber Security Consultant)
| Suisse Cyber Security
| www.suissecybersecurity.ch