Cybergangster agieren meist nach dem Giesskannenprinzip

Wer regelmässig Nachrichten hört oder liest, bekommt schnell den Eindruck, bei jedem Click ins Internet könnte man in einen Hinterhalt von Cyberkriminellen tappen. Mithilfe der Technik und vor allem des gesunden Menschenverstandes lassen sich aber die meisten Attacken abwehren.

Die Devise der Cyberkriminellen: einfach mal probieren. *Bild: Unsplash – Jefferson Santos*

Die Gefahren lauern überall. Berichte über Hacker, die die Computersysteme ganzer Firmen und öffentlicher Einrichtungen lahmgelegt haben, sind alltäglich geworden. Logisch giessen dann auch noch einige Anbieter von IT-Sicherheitssystemen Öl ins Feuer. Es genügt, tatsächlich passierte Angriffe öfters aufzuwärmen, um die IT-Nutzer ganz gehörig ins Schwitzen zu bringen.

Überbeissen hilft allerdings auch nicht wirklich weiter. Kühlen Kopf bewahren umso mehr. Nach Angaben von Max Klaus, stv. Leiter der Melde- und Analysestelle Informationssicherung des Bundes (MELANI), erfolgen die meisten Angriffe der Cyberkriminellen schlicht nach dem Giesskannenprinzip. Einfach einmal probieren. Grundsätzlich gebe es also keine grossen Unterschiede bezüglich Angriffsformen auf Privatpersonen oder auf Unternehmen und Verwaltungen. Im privaten Bereich sind es häufig immer wieder Phishingangriffe auf E-Banking-Kunden. Das offenkundige Ziel hier: Der User soll auf einen Link klicken und auf einer gefälschten Webseite Log-in-Daten, Passwörter oder gar Kreditkartenangaben eingeben. Das Perfide: Die Mails sehen oft genau so aus, als kämen sie von Banken, Onlineshops, iTunes oder sonstigen Websites mit persönlichen Konten.

Das einzig Richtige hier: Man sollte nie, absolut nie zur Eingabe von Logindaten auf einen Link in einem Mail klicken. Die meisten Unternehmen werden auch niemanden per Mail auffordern, das zu tun.

Private und Organisationen können auch von Kryptotrojanern betroffen sein. Krypto- oder Verschlüsselungstrojaner sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann.

So sollten sich Firmen und Verwaltungen zusätzlich schützen

Wie Privatpersonen werden auch Gemeinden und Firmen am häufigsten durch Giesskannenangriffe ins Visier genommen. Teilweise gibt es aber sehr gezielte Angriffe auf Unternehmen und Verwaltungen, dies zum Beispiel im Rahmen von Wirtschaftsspionage. Solche gezielten Angriffe erfolgen in der Regel sehr professionell und sind daher äusserst schwierig zu erkennen. In letzter Zeit gab es zudem grössere Wellen von Angriffen mit Kryptotrojanern gegen Schweizer Unternehmen, mit denen deren Computersysteme lahmgelegt werden sollten oder wurden.

Im geschäftlichen Umfeld reichen die oben beschriebenen technischen Abwehrmassnahmen allein nicht mehr aus, betont Max Klaus, der stellvertretende Leiter von MELANI. Es sei unumgänglich, die technischen Vorkehrungen auch durch organisatorische Massnahmen zu ergänzen, zum Beispiel durch

- die Regelmässige Sensibilisierung der Mitarbeitenden im Umgang mit den verschiedensten Diensten im World Wide Web.
- eine konsequente Benutzerverwaltung. Nicht alle Mitarbeitenden brauchen weitreichende Administratorenrechte. So ist es beispielsweise nicht sinnvoll, dass ein Mitarbeitender der Einwohnerkontrolle Zugriff auf die Lohnbuchhaltung hat. Bei Austritten aus der Firma oder auch bei internen Stellenwechseln sind diese Rechte unverzüglich entsprechend anzupassen.
- ein Business Continuity Management (BCM): Gemeint ist hier ein Notfallplan, der sicherstellt, dass auch weitergearbeitet werden kann, wenn die IT aus irgendwelchen Gründen vorübergehend nicht zur Verfügung steht. Ein Ausfall der IT muss nicht unbedingt die Folge eines Cyberangriffs sein. Auch Umwelteinflüsse wie Sturm, Feuer oder Wasser können einen solchen Ausfall herbeiführen.
- Ein stimmiges Kommunikationskonzept: Es muss unbedingt sichergestellt werden, wie eine Verwaltung im Fall eines Cyberangriffs die Betroffenen informiert. Wer genau ist verantwortlich, und wer informiert in welcher Form und zu welchem Zeitpunkt?

Essenziell: «Das Business Continuity Management und das Kommunikationskonzept müssen unbedingt vor Entdecken eines Cyberangriffs erstellt sein», unterstreicht Klaus. «Ist ein Angriff erfolgt, bleibt keine Zeit mehr für die Erstellung dieser Konzepte.»

Fredy Gilgen

Microsoft ruft an und will den PC reparieren
Ein zum Glück nicht mehr so häufig verwendeter Trick: Via Telefon meldet sich eine Mitarbeiterin von Microsoft (oder einer anderen bekannten IT-Firma) und berichtet über verdächtige Aktivitäten. Um Schaden zu vermeiden, solle ein Programm installiert werden. Dank diesem Programm hätten die Täter dann vollen Zugriff auf den Computer.
Nützlich zu wissen: Softwarefirmen melden sich nie auf diese Weise per Telefon. Unbedingt sofort aufhängen. Wer unsicher ist, sollte selber zurückrufen, über jene Kontaktnummer, die man selber in den Unterlagen hat oder die im Telefonbuch steht. Falls der falsche Supportmitarbeiter Zugriff auf den Computer hatte, sollte dieser von einer Fachperson neu installiert werden. Die Kreditkarte sollte gesperrt werden.
Es ist offensichtlich: Auch die Cyberkriminellen lernen rasch dazu. Generell werden die Angriffe immer professioneller. Der auf Informationssicherheit spezialisierte emeritierte Professor Hannes Lubich (siehe Interview) sieht die Ausbildung der Hacker gar als «grösste Hochschule der Welt». Vor allem weniger IT-affine Personen bekunden deshalb mehr und mehr Mühe, seriöse Mitteilungen von Nachrichten mit betrügerischen Absichten zu unterscheiden. Phishingmails beispielsweise werden heute meistens in perfektem Deutsch und teilweise sogar mit personalisierter Anrede verschickt.
Wie kann man sich am besten schützen? Wer die Türen schliesst und den Schlüssel dreht, der hat schlicht weniger ungebetene Gäste. Wichtig ist es also, auch im Umgang mit der Informationstechnologie elementarste Sicherheitsvorkehren einzuhalten. Nach der Überzeugung von Max Klaus bietet im privaten Umfeld der gesunde Menschenverstand gepaart mit den gängigen technischen Massnahmen wie Updates, Datensicherung, Firewall, Antivirus usw. bereits einen sehr guten Grundschutz. «Ist man sich nicht sicher, ob eine Nachricht seriös oder betrügerisch ist, löscht man diese Nachricht am besten. Angreifer nehmen sich äusserst selten die Zeit zum Nachfassen, wenn ein potenzielles Opfer nicht innert nützlicher Frist auf eine Nachricht reagiert. Seriöse Absender werden dies jedoch mit grösster Wahrscheinlichkeit tun», so Klaus.
Dann die Passwortfrage: Bei allen Onlinediensten, also E-Banking, Shops, Foren, E-Mail usw., sollten unterschiedliche Passwörter verwendet werden. Für die Aufbewahrung dieser Passwörter empfehlen sich Passwortsafes oder -manager, von denen es auch viele kostenlose Versionen gibt.

Fredy Gilgen

Der Druck zur Erweiterung des Dienstleistungsangebots erhöht das Risiko: Interview mit Hannes Lubich, emeritierter Professor an der Fachhochschule Nordwest-Schweiz FHNW

Herr Lubich, was sind die Gefahren und Risiken, denen eine Gemeindeverwaltung aktuell am stärksten ausgesetzt ist?
Lubich: Eine Gemeinde verwaltet einerseits sensitive Daten, auf die illegal Zugriff genommen werden könnten, andererseits auch Finanzmittel, auf die es ein Angreifer abgesehen haben könnte. Darüber hinaus kann eine Gemeinde natürlich auch auf politischer Ebene angegriffen werden.

Wie geschieht dies konkret?
Lubich: Etwa durch Falschinformationen zu Projekten, Finanzen, Wahlen oder Abstimmungen. Anvisiert werden sowohl Mitarbeitende der Gemeindeverwaltung wie Politiker, Lieferanten oder auch die technischen Zugänge, die oft zusätzlich zu den kantonalen, meist gut abgesicherten Infrastrukturen lokal betrieben werden. Daneben können natürlich auch Gemeindeverwaltungen durch Datenverschlüsselungen, sogenannte Crypto Locker, und Ähnlichem erpresst werden.

Gibt es Statistiken über Angriffe auf Gemeindeverwaltungen?
Lubich: In den jeweiligen kantonalen Informatikorganisationen gibt wohl einige Erkenntnisse dazu, aber systematisch erhoben und übergreifend konsolidiert werden diese Daten nicht. Zudem wird es wohl auch eine gewisse Dunkelziffer nicht gemeldeter Vorkommnisse geben. Nicht erfasst werden können erfolgreiche Angriffe oder Angriffsversuche, die gar nicht erkannt und somit auch nicht gemeldet werden.

Mit welchen Trends im Bereich Cyberrisiken muss eine Gemeinde künftig rechnen?
Lubich: Hier sind die zunehmende Auslagerung von Diensten in Cloud-Lösungen sowie der ständige Druck zur Erweiterung des Dienstleistungsangebots für die Einwohner und die politischen Funktionsträger zu nennen. Die Bewirtschaftung der Schnittstellen wird zudem immer komplexer und das Interesse der organisierten Kriminalität für Daten und Geld nimmt stetig zu.

Wie sollten sich die Gemeinden schützen?
Lubich: Gemeindeverwaltungen, die nicht zu 100 Prozent auf Systemen, Applikationen und Netzwerken des Kantons basieren, brauchen zwingend Dispositive für die Risikoerkennung und das Risikomanagement. Unbedingt vorhanden sein muss immer auch ein ausreichend gut definierter und beübter Plan B für den Notfall, um die wichtigsten Dienste auch im Fall von Angriffen aufrechterhalten zu können.

Ein eigenes Sicherheitscenter aufzubauen, ist wohl nur für die grössten Gemeinden eine Option. Welche Lösungen bieten sich für kleinere Gemeinden an?
Lubich: Kleine Gemeinden können je nach Kanton auf Dienste der zentralen Informatikdienste zurückgreifen. Sind solche Dienste nicht vorhanden, bieten kommerzielle SOC-Betreiber auch Dienstleistungspakete an, die bezüglich Leistungsumfang und Preisgestaltung für Gemeinden durchaus realistisch sind. In allen Fällen muss die Gemeinde aber ihren Teil der Verantwortung weiterhin übernehmen und hat auch die nicht delegierbare «Governance»-Verantwortung.
Dies gilt etwa für die Identifikation von Ansprechpartnern auch ausserhalb der Bürozeiten, eine ausreichend rasche Intervention oder die Definition der Abläufe bei erkannten Angriffen.

Interview: Fredy Gilgen