KANTON AARGAU
Departement
Volkswirtschaft und Inneres

Scannen Sie den QR-Code, um direkt auf diese Webseite zu gelangen

Auch Schweizer KMU sind Cyber-Attacken ausgesetzt

Gastbeitrag von Franco Cerminara, Chief Consulting Officer, InfoGuard AG

Nicht nur Grossunternehmen wie Banken, Versicherungen, Rüstungsbetriebe oder die Pharma-Industrie sind von den Gefahren aus dem Internet bedroht. Auch Schweizer KMU sehen sich einer wachsenden Zahl von Cyber-Attacken ausgesetzt. Es stellt sich nicht mehr die Frage, «ob» das eigene Unternehmen angegriffen wird, sondern nur noch «wann» und «wie». Dabei sind die Folgen oft schwerwiegender als die Attacke selbst. Imageschäden und enorme Kosten entstehen insbesondere durch Identitäts- und Datendiebstahl, Cyber-Erpressung oder gezielte Angriffe auf Produktions- und IT-Systeme mit dem Ziel, diese lahmzulegen.

Auf leisen (Hacker-)Sohlen…

Die Mittel und Methoden der Hacker sind heute sehr vielfältig – und sie werden immer professioneller. Vielfach sind Schlüsselpersonen eines Unternehmen Ziel des Cyber-Angriffs. Im Vorfeld spionieren die Cyber-Kriminellen teilweise über Wochen und Monate hinweg das im Fokus stehende Unternehmen aus. Es werden möglichst viele Informationen über das Umfeld zusammengetragen, um sich gezielt vorbereiten zu können. Gesammelt werden Informationen zu Betätigungsfeldern, Schlüsselposten, Telefonnummern, E-Mail-Adressen etc. Dabei nutzen die Betrüger typischerweise Informationen aus offenen Quellen, wie sie auf der Webseite jedes Unternehmens zu finden sind oder auch aus den sozialen Netzwerken. Diese Informationen werden durch aktive

Recherche ergänzt, indem die Betrüger unter Täuschung von Identitäten mit dem Unternehmen via E-Mail oder Telefon Kontakt aufnehmen und so versuchen, direkt an Informationen zu gelangen. Anschliessend beginnt der eigentliche Angriff.

So gehen Cyber-Kriminelle vor

Doch welche Arten von Attacken drohen konkret, und über welche Einfallstore gelangen die Cyber-Kriminellen in das Unternehmen? Bei den folgend aufgezählten Angriffsmethoden handelt es sich lediglich um die wohl bekanntesten Varianten und bilden daher nur einen kleinen Ausschnitt ab:

- **Phishing:** Phishing-Mails sind in der Regel E-Mails, die im Layout eines seriösen Anbieters – oft auch bekannte Unternehmen – getarnt sind. In Wahrheit sind es jedoch bösartige Nachahmungen, die den Empfänger dazu bringen sollen, persönliche Informationen wie Kreditkarten-Daten oder Passwörter preiszugeben.
- **Schadsoftware in E-Mails:** E-Mails sind immer noch der häufigste Verbreitungsvektor für Schadsoftware. Immer wieder versenden Betrüger E-Mails, die die Opfer dazu verleiten sollen, den Anhang zu öffnen und die Makro-Funktion zu aktivieren. Ziel ist es, die Schadsoftware auf dem Computer zu installieren, die danach automatisch auf Informationen zugreift oder beispielsweise das System lahmlegt.
- **Schadsoftware auf Webseiten:** Allein durch den Besuch einer Webseite wird der Computer des Opfers mit Schadsoftware infiziert, indem sie vorhandene Schwachstellen des Browsers ausnutzt. Man spricht in diesem Fall von Drive-by-Infection.
- **Schadsoftware auf USB-Sticks oder anderen Speichermedien:** Hier wird die Schadsoftware durch das Anschliessen eines fremden USB-Sticks installiert.
- **Verschlüsselungstrojaner:** Dateien auf dem Computer sowie auf den verbundenen Netzlaufwerken werden verschlüsselt und somit für das Opfer unbrauchbar gemacht. Die Trojaner können als Anhang in E-Mails, per USB-Stick oder via infizierte Internetseiten auf den Rechner gelangen.
- **CEO-Betrug:** Im Namen des CEOs wird die Buchhaltung oder der Finanzdienstleister in einer E-Mail angewiesen, eine Zahlung an den Betrüger auszulösen.
- **Social Engineering:** Diese Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus mit dem Ziel, an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Aktionen zu bewegen. Ein solcher Angriff kann beispielsweise auch physisch geschehen, in dem sich eine fremde Person als neuer Mitarbeiter ausgibt um, so Zutritt zum Gebäude zu erhalten.
- **Gefälschte Supportanrufe:** Betrüger geben sich meistens als Support- oder Helpdesk-Mitarbeiter aus und versuchen auf diesem Weg, eine Schadsoftware auf dem Rechner des Opfers zu installieren.

Setzen Sie präventive Sicherheit

Auch wenn es keinen vollständigen Schutz gibt: Wer die folgenden Ratschläge beherzigt, kann immerhin die Wahrscheinlichkeit von Cyber-Attacken reduzieren – oder zumindest die Folgen abfedern. Der erste Schritt ist dabei, Risiken zu erkennen und sich diesen zu stellen.

- Aufbau eines **Cyber Security Frameworks** und Festlegung von Prozessen, Aufgaben, Rollen und Verantwortlichkeiten.
- **Identifikation** Ihres spezifischen **Bedrohungspotentials** durch Cyber-Attacken.
- Durchführung **simulierter Cyber-Attacken**, regelmässige **Penetration Tests** und spezifische **Compliance Assessments**.
- Schutz Ihrer ICT-Infrastruktur durch **erprobte Sicherheitslösungen**.
- **Sensibilisierung** Ihrer **Mitarbeitenden** hinsichtlich dem Umgang mit kritischen oder sensiblen Daten.
- **Erkennung** von **Cyber-Attacken** und die rasche **Reaktion** bei Sicherheitsvorfällen.
- Sicherstellung einer zeitnahen **Wiederherstellung** des **Geschäftsbetriebs** nach einer Attacke.

Fazit: Es kann jeden treffen

Jedes KMU muss sich mit den Themen Cyber Security und Defence auseinandersetzen und den drei Dimensionen der IT-Sicherheit – Technologie, Prozesse und Mensch – das nötige Gewicht beimessen. Mit dem Cyber Security-Ratgeber für KMUs erlangen Sie eine angemessene Cyber Security. Erfahren Sie mehr zu den Schutzmöglichkeiten vor den zunehmenden Gefahren der Cyber-Welt. Haben Sie Interesse? Dann laden Sie unseren kostenlosen Cyber Security-Ratgeber herunter!

Über InfoGuard

Die InfoGuard AG ist spezialisiert auf umfassende Cyber Security. Zu ihren Kompetenzen zählen massgeschneiderte Dienstleistungen im Bereich der Sicherheitsberatung und Security Audits sowie in der Architektur und Integration führender Netzwerk- und Security-Lösungen. Aus dem ISO 27001 zertifizierten Cyber Defence Center erbringt InfoGuard vielfältige Cyber Defence Services sowie individuelle Cloud-, Managed- und Support Services. InfoGuard hat ihren Hauptsitz in Baar / Zug und eine Niederlassung in Bern.

(vom 24. April 2018)

Franco Cerminara

Chief Consulting Officer

InfoGuard AG