Medienmitteilung vom 1. Mai 2023

Informationssicherheit ist mehr als Cyber Security

Starke Passwörter, regelmässige Backups, geprüfte Software und sichere Netzwerke sind nur die Basis, wenn es um Informationssicherheit geht. Sicher sind sensible Informationen und Geschäftsgeheimnisse nur, wenn die Cyber Security auch die physische Welt und den Faktor Mensch mitberücksichtigt. In diesem Bereich verhalten sich viele Organisationen naiv. Wenn Mitarbeitende leichtsinnig Informationen teilen oder vermeintliche Handwerker unbehelligt Wanzen installieren können, nützt das beste Cyber-Security-Konzept nichts.

Das Einmaleins der üblichen Cybersicherheit ist bekannt – keine Links in verdächtigen Mails anklicken, Zugangsdaten geheim halten, starke Passwörter, aktualisierte Geräte und sichere Onlineverbindungen nutzen. Das wissen auch kriminelle Hackergruppen, aggressive Konkurrenzorganisationen und Wirtschaftsspione. «Heute wird die Schwachstelle Mensch via Social Engineering am häufigsten ausgenutzt, weil die technischen Massnahmen flächendeckende, günstige Online-Massenangriffe immer zuverlässiger verhindern», sagt Chris Eckert, Sicherheitsexperte und CEO der Swiss Business Protection AG, an einer Veranstaltung der OST – Ostschweizer Fachhochschule.

Das Repertoire beschränkt sich heutzutage aber nicht nur auf Social Engineering. Wenn es darum geht, an Informationen zu gelangen setzen Angreifer unterdessen auch auf günstig verfügbare Spionagetechnik, die früher nur staatlichen Geheimdiensten zur Verfügung stand. Ein umfassender Schutz vor Informationsdiebstahl erfordert heute deshalb mehr als nur eine gute IT-Sicherheit.

Schadenspotenzial beeinflusst Schutzmassnahmen kaum

Dem möglichen Schadenspotenzial durch die neuen Angriffsmöglichkeiten gegenüber stehen paradoxe Zahlen: Obwohl die Schäden durch erfolgreiches Social Engineering, Sabotage, Daten-Erpressung oder Lauschangriffe mit Minikameras- und -mikrofonen weltweit in den dreistelligen Milliardenbereich gehen und mehr als 75 Prozent aller angegriffenen Unternehmen konkrete Schäden durch solche Angriffe erleiden, holen sich nur rund 20 Prozent aller Unternehmen in der Schweiz professionelle Hilfe für den Schutz vor Attacken, für deren Abwehr ihnen eigenes Know-how fehlt.

Den Hintergrund verortet Eckert in einem falschen Sicherheitsgefühl: «Nicht nur offensichtliche Ziele wie Militärorganisationen oder internationale Konzerne sind für Angreifer interessant. Jede Einzelperson mit peinlichen Fotos oder Zugang zu Firmennetzwerken und jedes Unternehmen vom Konzern mit begehrten Produkt-Bauplänen bis hin zum Dorfmetzger mit seinem geheimen Wurstrezept hat Daten, die sich weiterverkaufen lassen oder die sie erpressbar machen.»

Kreative Angriffsmethoden

Entsprechend kreativ gehen Wirtschaftsspione und Kriminelle vor. Der technische Fortschritt hat dazu geführt, dass heute kleine unauffällige Wanzen für wenige hundert Franken monatelang hochqualitatives Ton- und Bildmaterial aufzeichnen können. Getarnt als USB-Ladegeräte, Kugelschreiber oder USB-Stick, versteckt im Lichtschalter oder in der Fernbedienung liefern sie zuverlässig Informationen, die sich zu Geld machen oder als Druckmittel verwenden lassen. Wenn so ein Gerät zum Beispiel von Angreifern während einem harmlos wirkenden, alltäglichen Verkaufsgespräch in einem häufig genutzten Besprechungsraum versteckt wird, nützt auch eine in

der digitalen Welt stark geschützte Videokonferenzanlage im Raum wenig – die Angreifer können anschliessend trotzdem monatelang alles mithören.

Doch es geht noch einfacher. Baustellen sind laut Eckert beliebte Angriffspunkte. Der Zutritt auf eine belebte Baustelle wird selten systematisch beschränkt. Wo viele untereinander unbekannte Handwerker arbeiten, fällt es kaum auf, wenn der vermeintliche Elektriker im Rauchmelder, hinter Steckdosen oder im Verteilerkasten noch eine kleine Wanze zusätzlich installiert. Zudem ist der steigende Anteil smarter internetfähiger Geräte ein zusätzliches Einfallstor: «Solche Geräte haben meistens bereits ein Mikrofon oder eine Kamera installiert, da muss man nicht mal noch extra etwas einbauen», so Eckert.

Cyber Security mit weiteren Massnahmen ergänzen

Neben einer grundsätzlich gut aufgestellten Cybersecurity und bezüglich Informationssicherheit gut geschulten Mitarbeitenden empfiehlt Eckert aufgrund der vielen Angriffsmöglichkeiten weitere Massnahmen von Hintergrund-Checks für Mitarbeitende mit Zugang zu sensiblen Informationen bis hin zur professionellen Wanzensuche – etwa nach einem Umzug in neue Geschäftsräume. Mit Thermokameras, Röntgengeräten und physischen Durchsuchungen lassen sich Wanzen oder technische Manipulationen häufig entdecken. Ebenfalls wichtig sei eine Sensibilisierung der Verantwortlichen für Informationssicherheit, dass sich die Angriffsmöglichkeiten nicht nur auf digitale Attacken beschränken.

((BILDLEGENDEN))

Methoden der Kriminalpolizei: Mit speziellen Chemikalien werden die Fingerabdrücke auf einem Glas sichtbar.

Eine Wärmebildkamera zeigt, wo im Hörsaal der OST Menschen sitzen.

((KASTEN))

Cyber Security als Weiterbildung

Cyber Security ist komplex, umfassend und ändert sich rasch, sowohl technologisch als auch politisch. Mit dem berufsbegleitenden Zertifikatskurs CAS Cyber Security bieten wir erfahrenen IT-Fachleuten die Möglichkeit, sich im Bereich Cyber Security zu spezialisieren. Die praxisorientierte Ausbildung ist auf die Technik fokussiert.

Für Rückfragen:

- Michael Breu, Kommunikation OST, +41 58 257 44 66, michael.breu@ost.ch