UBS

Sind Sie sicher?

Welchen Cyberrisiken Ihr Unternehmen ausgesetzt ist – und wie Sie sich dagegen schützen

E-Mail und Internet sind seit jeher auch ein Tummelfeld krimineller Elemente. Sie nutzen das Web, um an vertrauliche Informationen zu gelangen, um Firmen zu erpressen oder um Geld von fremden Konten zu stehlen. Technische Mittel bieten einen grundlegenden Schutz – Cyberkriminelle nutzen deshalb gerne menschliches Versagen als Türöffner für fremde Systeme. In diesem Papier beschreiben wir die aktuellen Cyberrisiken und sagen Ihnen, wie Sie damit umgehen sollten.

Was muss ich über Cyberrisiken wissen, welche Gefahren bestehen?

Cyberkriminelle brauchen oft nur wenige Minuten, um in ein Netzwerk einzudringen, Schaden anzurichten und wieder zu verschwinden.

Die Statistik zeigt, dass die Zahl erfolgreicher Cyberattacken laufend steigt; betroffen sind Firmen aller Grössen. Technische Massnahmen bilden die Basis eines jeden Abwehrdispositivs gegen Cyberrisiken – Firewalls, Virenschutzprogramme und Ähnliches, die laufend aktualisiert werden und dem Stand der Technik entsprechen. Doch immer häufiger nutzen Cyberkriminelle nicht technische Schwachstellen aus, sondern verschaffen sich den Zugang zu Firmennetzwerken durch gezielte Ansprache von Mitarbeitern – der «Faktor Mensch» wird zum entscheidenden Schwachpunkt. Dabei verwenden sie verschiedene Methoden. Die wichtigsten:

- **Social Engineering:** Kriminelle versuchen Mitarbeiter so zu beeinflussen, dass sie vertrauliche Informationen preisgeben – häufig am Telefon. Dabei nutzen die Angreifer öffentlich verfügbare Informationen (zum Beispiel aus dem Facebook- Profil des Angerufenen), um an vertrauliche Geschäftsinformationen oder Benutzerdaten zu gelangen.

- **Phishing:** Die Angreifer versuchen, mittels gefälschter Webseiten oder E- Mails an vertrauliche Informationen wie Benutzernamen oder Passwörter zu gelangen. Mit dieser gestohlenen Identität manipulieren die Kriminellen alsdann Daten oder lösen Überweisungen aus.

- **CEO-Scam:** Mitarbeiter eines Unternehmens werden per E- Mail von einem realen oder fiktiven Manager aufgefordert, Überweisungen zu veranlassen. Ein wichtiger Aspekt des CEO- Scams ist der Verweis auf Dringlichkeit und Verschwiegenheit; auch verwenden die Cyberkriminellen oft gefälschte Telefonnummern, um mögliche Bedenken auszuräumen.

- **Schadsoftware (Malware):** Angreifer können mit Malware verschiedene Ziele verfolgen. Die häufigsten drei sind:
  - Zutritt in ein geschütztes System (Beispiel: trojanisches Pferd, Backdoor)
  - Zugang zu vertraulichen Informationen (Keylogger, Spyware)
  - Löschen oder Verschlüsseln von Daten (Virus, Ransomware)

Seit einiger Zeit beobachten wir eine Zunahme der Angriffe durch Ransomware: Alle Daten auf dem betroffenen Rechner werden verschlüsselt und somit unbrauchbar. Für die Entschlüsselung verlangen die Kriminellen ein Lösegeld (englisch: ransom); wie bei herkömmlicher Erpressung gibt es keine Garantie, dass die Daten nach Bezahlen des Lösegeldes entschlüsselt und wieder brauchbar werden.

Auch trojanische Pferde werden häufig eingesetzt. Dabei handelt es sich um eine Malware, die als Anhang einer E- Mail verschickt wird – oft in Form einer Word- oder Excel- Datei. Beim Öffnen des Anhangs installiert sich die Schadsoftware auf dem Rechner. Die Angreifer erhalten so einen Fernzugang auf den Server und können zum Beispiel vertrauliche Daten herunterladen oder Geld überweisen.

Wie kann ich mich und mein Unternehmen gegen Cyberrisiken schützen?

Aufmerksamkeit ist der beste Schutz gegen Internetkriminelle. Befolgen Sie und Ihre Mitarbeitenden die folgenden Tipps, so können Sie viel Unheil abwenden.

- Klicken Sie nie auf einen Link in einer E- Mail und öffnen Sie keine Anhänge, wenn Sie den Absender nicht kennen und/oder Zweifel haben an der Echtheit des Absenders.
- Deaktivieren Sie unter keinen Umständen Sicherheitsmechanismen (zum Beispiel eine Makrosperre), wenn Sie beim Öffnen einer Datei dazu aufgefordert werden – informieren Sie stattdessen umgehend den Sicherheitsverantwortlichen oder den Systemadministrator Ihres Unternehmens.
- Antworten Sie nie auf E- Mails von unbekannten und/oder unerwarteten Absendern. Mit Ihrer Antwort signalisieren Sie einem potenziellen Angreifer, dass die E- Mail- Adresse benutzt wird, worauf er seine Attacken fortsetzen dürfte.
- Reagieren Sie nicht auf E- Mails, die Ihnen entweder materielle Vorteile versprechen («Sie haben gewonnen!»), Sie durch Dringlichkeit zu unüberlegten Aktionen motivieren wollen («Handeln Sie sofort!») oder die Ihnen Angst machen wollen («Ihr Konto wird gesperrt!»).
- Überprüfen Sie Links in E- Mails, bevor Sie darauf klicken: Wenn Sie mit dem Mauszeiger über den Link fahren, sehen Sie die verlinkte Internetadresse. Stimmt diese mit dem angezeigten Text überein? Achten Sie genau auf die Schreibweise; bei URL mit mehreren durch Punkte getrennten Wörtern ist immer der Begriff unmittelbar vor dem Suffix (.ch, .com, .net) entscheidend.
- Werden Sie misstrauisch, wenn Inhalt und Stil einer E- Mail nicht zum (vorgeblichen) Absender passen. Ein seriöses Unternehmen wird Ihnen keine E- Mails in schlechtem Deutsch mit vielen Schreibfehlern schicken.
- Seien Sie sehr zurückhaltend mit persönlichen Informationen auf öffentlich zugänglichen Plattformen wie Facebook oder Twitter.

Haben Sie eine E- Mail erhalten, die Ihnen verdächtig vorkommt und die in einem Zusammenhang mit UBS steht – zum Beispiel als angeblichem Absender? Bitte senden Sie uns die E-Mail mit diesem Formular. Stellen Sie bitte sicher, dass diese E- Mail keine persönlichen Daten wie Kontoangaben enthält.

Wo finde ich weitere Informationen zu aktuellen Cyberrisiken?

Staatliche Stellen informieren auf ihren Webseiten unter anderem über die aktuelle Gefahrenlage und bieten Anleitungen zum Schutz gegen die gängigsten Cyberrisiken.

MELANI – Melde- und Analysestelle Informationssicherung des Bundes. Sie finden auf der Website eine Übersicht der aktuellen Gefahren, Tipps zum Schutz und weiterführende Informationen. Die Website wendet sich an KMU und Privatpersonen in der Schweiz. melani.admin.ch

Europol – diese englische Webseite enthält wertvolle Anleitungen zum Schutz vor Identitätsdiebstahl, Kartenbetrug, Malware und vieles mehr. europol.europa.eu > Media Corner > Crime Prevention

ENISA – Europäische Agentur für Netz- und Informationssicherheit. Auf dieser englischen Webseite erwartet Sie eine breite Auswahl an Inhalten zum Thema Cyberrisiken. enisa.europa.eu/topics