UNIT Newsletter
Beitrag / Leitartikel

Cyberangriffe: Der Mensch bleibt Einstiegstor Nummer 1

Kennen Sie diese Tage nicht auch? Ein Meeting folgt auf das andere, das Telefon steht nicht still, Baupläne müssen abgenommen werden. Dann steht ein Besuch auf der Baustelle an. Das Problem mit den Lieferengpässen muss auch noch geklärt werden und nebenbei müssen auch noch E-Mails gelesen und beantwortet werden. Und nun mal Hand aufs Herz: Schauen Sie in diesen Situationen immer ganz genau hin und prüfen jede E-Mail auf Ihre Authentizität? Nein? Das ist verständlich, kann aber gefährlich werden. Denn ein falscher, unüberlegter Klick reicht aus, um Computer, Netzwerke oder im schlimmsten Fall das ganze Unternehmen lahmzulegen.

Der Großteil der Cyberangriffe wird immer noch von Menschen verursacht. UNIT-Berufshaftpflichtkunden haben jetzt die Möglichkeit, einfach herauszufinden, ob Mitarbeitende Phishing erkennen und nicht den gefährlichen Klick machen. Völlig risikofrei und kostenlos - in Kooperation mit dem Cybersicherheitsunternehmen Perseus.

Aktuelle Situation

Cyberattacken sind nicht erst seit gestern eines der größten Geschäftsrisiken für deutsche Unternehmen. Das aktuelle Allianz Risk Barometer 2022 zeigt, dass Cyberattacken an erster Stelle stehen, gefolgt von Betriebsunterbrechungen - eine häufige Folge von Cyberattacken. Vor allem die Dynamik und Flexibilität, mit der Cyberkriminelle ihre Angriffswellen planen und durchführen, tragen zu dieser Situation bei. Im Jahr 2021 wurden zum Beispiel 144 Millionen neue Malware-Programme registriert - das entspricht 394.000 neuen Schadprogrammen pro Tag.

Jeder steht im Fokus

Inzwischen sind 9 von 10 Unternehmen von Datendiebstahl, Sabotage und Spionage betroffen (Bitkom). Kein Unternehmen ist sicher. Jede und jeder kann zum Opfer werden, denn kriminelle Hacker werfen ihre Köder willkürlich aus. So greifen sie manche Unternehmen ganz gezielt an. Andere geraten durch eine großflächig angelegte Angriffswelle ins Visier. Mit einem durchschnittlichen Schaden in Höhe von 72.000 € (Hiscox), kann das für das ein oder andere Unternehmen gravierende Folgen haben.

Krisen verschärfen die Lage

Die letzten zwei Jahren haben das Geschäft der Cyberkriminellen noch befeuert. Die Corona-Pandemie zwang Unternehmen seine Mitarbeitenden ins Home Office - oftmals ohne ausreichende Instruktionen, wie ein sicherer Arbeitsplatz in den eigenen vier Wänden auszusehen hat. Kriminelle Hacker hatten so leichtes Spiel. Auch der Ausbruch des Kriegs in der Ukraine trägt dazu bei, dass sich die Lage immer weiter anspannt. Denn neben dem eigentlichen Kriegsschauplatz, wird der Kampf auch im Cyberspace ausgetragen. Nach wie vor muss mit Denial-of-Service (DDoS) Angriffen, mit der Verbreitung von Falschinformationen sowie Phishing-Angriffen gerechnet werden.

Was ist Phishing und wie kann man sich schützen?

So bleibt Phishing ganz oben auf der Liste der häufigsten Cyberangriffe. Cyberkriminelle versuchen, das Vertrauen von Menschen zu gewinnen, indem sie vorgeben, eine bekannte Person oder Organisation zu sein, und sie dazu bringen, bereitwillig Informationen preiszugeben. Dies geschieht häufig über eine E-Mail. Phishing kann aber auch per Telefonanruf (Vishing), per SMS (Smishing) oder sogar per QR-Code (Quishing) erfolgen. Alle Formen haben jedoch eines gemeinsam. Der Mensch steht im Fokus und wird dazu verleitet, sensible Daten zu teilen.

Menschliche Firewall: Beste Schutzmaßnahme

Auch wenn der Mensch als Einfallstor Nummer eins gilt, so ist er doch auch der beste Schutzschild für Unternehmen, um sich gegen Cyberangriffe zu wehren - wenn er für die Gefahren aus dem Internet sensibilisiert ist. Um Unternehmen nachhaltig gegen Cybergefahren zu wappnen, muss Cybersicherheit fest in der Unternehmenskultur verankert werden. Neben ausreichenden technischen Schutzmaßnahmen, wie einer aktiven Firewall und ständig aktualisierter Antivirensoftware, müssen die Mitarbeiter geschult und auf die Angriffsmethoden und -muster krimineller Hacker vorbereitet werden.

Testen Sie es aus!

Um herauszufinden, ob UNIT-Berufshaftpflichtkunden gut aufgestellt und ihre Mitarbeitenden ausreichend geschult sind, um Phishing zu erkennen und richtig zu reagieren, bietet das Berliner Cybersicherheitsunternehmen Perseus Technologies in Kooperation mit UNIT Versicherungsmakler den Phishing Check an. Dabei werden

simulierte, realitätsnahe Phishing-E-Mails versendet. An diesem Test kann jedes Unternehmen teilnehmen. In wenigen Schritten werden das Unternehmen angelegt, Mitarbeitende zu dem Phishing Check hinzugefügt und die Simulation gestartet. Insgesamt werden bis zu drei Phishing-E-Mails versendet. Klickt ein Mitarbeitender auf eine der Phishing-Simulationen, wird der Test gestoppt und gilt als nicht bestanden. Erkennen Ihre Mitarbeitenden den Phishing-Versuch, ist der Test nach 7 Werktagen mit einem positiven Ergebnis beendet.

Keine Angst: Der Phishing-Check stoppt da, wo es in der Realität gefährlich wird. Verschaffen Sie sich einen Einblick, wie sicher Ihr Unternehmen wirklich ist - ohne Risiko und kostenlos. Neugierig geworden? Melden Sie sich gern bei Matthias Lange, Senior Director Broker bei Perseus Technologies unter: matthias.lange@perseus.de

Über Perseus

Die Perseus Technologies GmbH wurde im September 2017 gegründet. Das Berliner Unternehmen verfolgt die Mission, Cyberrisiken für alle beherrschbar zu machen und richtet sich dabei im Besonderen an Unternehmen. Ziel des mitarbeiterzentrierten Angebots von Perseus ist die Etablierung einer langfristigen Cybersicherheitskultur. Das Perseus-Konzept beinhaltet eine Cybersicherheits-Risikobewertung, ein umfassendes Cyber-Präventionsangebot mit Online-Trainings für Mitarbeitende und automatisierten Phishing-Simulationen sowie eine 24/7-Cybernotfallhilfe.

Das Cybersicherheitsunternehmen arbeitet mit rund 50 % der auf dem deutschen Markt tätigen Cyberversicherern - teilweise oder ganzheitlich - in den Bereichen Prävention, Notfallmanagement oder Risikobewertung zusammen.

Die über 60 Mitarbeiterinnen und Mitarbeiter kommen aus 20 Nationen und arbeiten gemeinsam im Fintech Hub H:32 in Berlin.