FACHBERICHT

LEICHTSINN FÖRDERT CYBER - ATTACKEN

PHISHING-ATTACKEN GEHÖREN ZU DEN GRÖSSTEN GEFAHREN DER IT-SICHERHEIT. WIE SICH KLEINE UND MITTELSTÄNDISCHE UNTERNEHMEN DEM PROBLEM STELLEN KÖNNEN.

Groß angelegte Angriffe auf Konzerne, Behörden und Einrichtungen stellen keine Seltenheit mehr dar, sondern sind fast alltäglich geworden. Die Coronakrise hat diesen Effekt noch verstärkt. Nach einem Report der European Union Agency for Cybersecurity vom 20. Oktober 2020 verursachten Angriffe über Mailpostfächer bereits 2019 Verluste in Höhe von rd. 26,2 Milliarden Euro. Allein 42,8 Prozent aller schadhaften Anhänge waren auf weitverbreitete Microsoft-Office Dokumente zurückzuführen. Zu Beginn der Pandemie (zwischen Ende Februar 2020 und Ende März 2020) nahmen die Phishing-Attacken laut ENISA allein innerhalb eines Monats um 667 Prozent zu.

Umfragen unterstreichen diese Aussagen: Laut Capterra, einer Bewertungsplattform für Unternehmenssoftware, empfinden Entscheider aus kleinen- und mittelständischen Unternehmen E-Mail-Phishing als größte Bedrohung. KMUs sind aufgrund teils unzureichender Sicherheitsmaßnahmen und ihrer Rolle als Zulieferer- bzw. Lieferant für große Unternehmen interessante Ziele für Angreifer geworden. Für sie ergibt sich somit die Herausforderung, mit (im Vergleich zu Großkonzernen) geringeren finanziellen Mitteln auf ein hohes Sicherheitsniveau zu kommen.

NIEDRIGE HEMMSCHWELLEN FÜR EINE INTERAKTION

Phishing-Attacken sind bei Cyberkriminellen besonders beliebt. Durch Betrug, Täuschung oder Irreführung ihrer Opfer versuchen diese dabei, vertrauliche und sensible Daten zu erlangen. Die Angriffsart ist unter dem Begriff Social Engineering einzuordnen. Dazu zählen neben Attacken per E-Mail auch das sogenannte USB-Dropping, gefälschte Textnachrichten via SMS oder fingierte Telefonanrufe.

Beim E-Mail-Verkehr enthält die Mail einen bösartigen Anhang oder Link zu einer „Fake"-Seite. Gewinne oder Erbschaften werden versprochen, es kann aber ebenso wie ein seriöses Angebot eines bekannten Lieferanten oder Kunden anmuten, sodass die Hemmschwelle für eine Interaktion durch das potenzielle Opfer möglichst gering ist. Manchmal werden gezielt bestimmte Benutzergruppen oder Unternehmenspositionen ins Visier genommen, um an besondere Berechtigungen oder Identitäten zu gelangen.

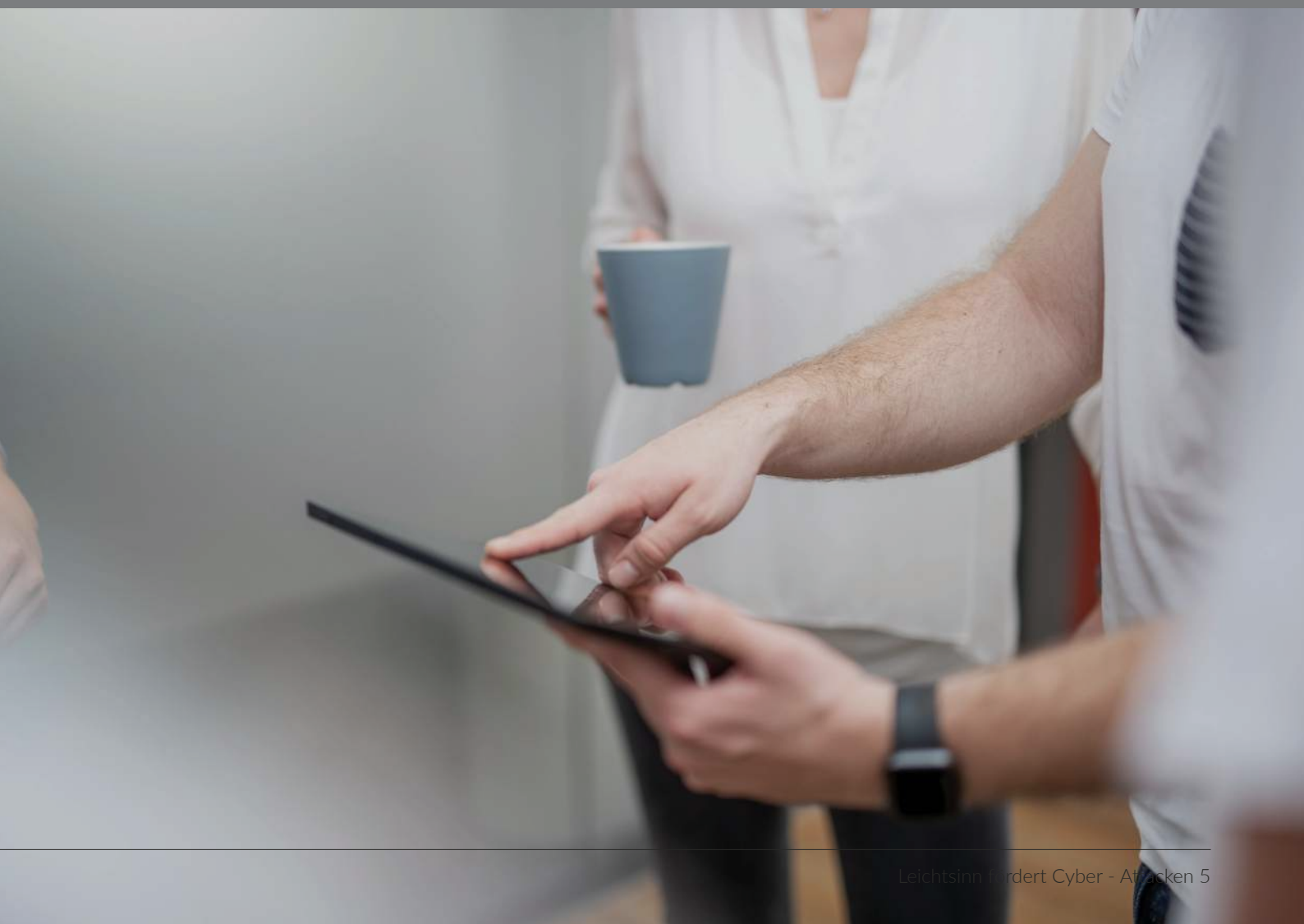
Letzten Endes ist der Faktor Mensch der ausschlaggebende Punkt. Wenn Mitarbeiter*innen als vermeintlich letzte Verteidigungslinie den E-Mail-Adressaten oder Inhalt nicht hinterfragen, sondern mit ihm interagieren, war die Attacke bereits erfolgreich. Die nun durch das sogenannte ‚Sniffing' (übersetzt: Schnüffeln) abgegriffenen Daten kann der Angreifer auslesen und für weitere kriminelle Aktivitäten nutzen. Im schlimmsten Fall werden Anmeldedaten abgezogen, die es dem Angreifer ermöglichen, auf weitere Unternehmensdaten zuzugreifen und in der Folge diese auch zu löschen, zu verschlüsseln oder im Dark Net anzubieten.

FINANZIELLE UND REPUTATIVE SCHÄDEN

Im Falle einer Verschlüsselung ist die verwendete Verschlüsselungstechnik in der Regel nicht einfach aufzulösen, um wieder Zugriff auf die Daten zu erlangen. Unternehmen, die ihre eigenen Daten nicht durch regelmäßig durchgeführte Backups gesichert haben, sollten die geforderten Auslösesummen dennoch auf keinen Fall zahlen und sich stattdessen von Experten beraten lassen, wie mit der Situation umzugehen ist. Denn fraglich ist, ob die Systeme nach der Zahlung des Lösegelds überhaupt entschlüsselt werden.

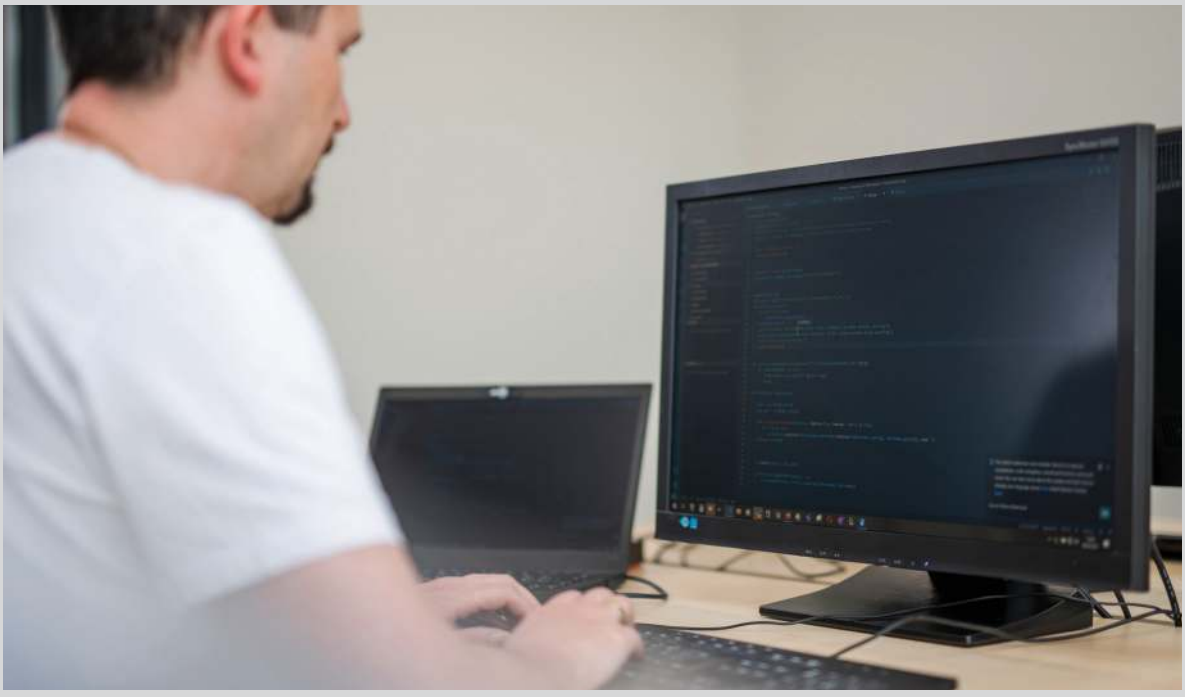
Solche Angriffe können für Unternehmen am Ende zu enormen finanziellen wie auch reputativen Schäden führen. Vertrauensverlust der Kunden, Kosten für den Know-how-Abfluss und die Beseitigung der Folgeschäden, Produktionsausfälle oder Auftragsstornierungen sind nur ein kleiner Überblick über mögliche Folgen, die bei einem erfolgreichen Cyber-Angriff entstehen können. Hinzu kommt, dass eine solche Datenpanne unverzüglich der zuständigen Aufsichtsbehörde gemeldet werden muss.

Cyberkriminelle werden auch zukünftig weiterhin auf Phishing-Attacken zurückgreifen, da die bereits vorhandene, technische Sicherheit vieler Systeme deren Angriffsmöglichkeiten reduziert und infolgedessen der Mensch inzwischen als schwächstes Glied in der Kette angesehen werden kann. Zudem sind derartige Attacken mit deutlich weniger Know-how und in größerem Ausmaß durchzuführen als klassische Hackerangriffe. Letztendlich ist auch noch die Erfolgsquote entscheidend: Unabhängig von der Unternehmensgröße reicht ein abgelenkter bzw. unvorsichtiger Angestellter aus, um folgenschwere Auswirkungen für das Unternehmen auszulösen. Bei 1.000 Beschäftigten muss nur eine Person (= 0,01%) mit der Phishing-Mail interagieren, um den Angreifern ausgeliefert zu sein. Eine solche Erfolgswahrscheinlichkeit gibt es in kaum einem anderen Angriffsszenario und wird dementsprechend unterschätzt – besonders im KMU-Bereich, wo Mittel und Ressourcen für IT-Sicherheit oft knapp bemessen sind und kein ausreichendes Know-how vorhanden ist.



EINFACHE GEGENMASSNAHMEN MÜSSEN NICHT TEUER

Das entscheidende Stichwort lautet: Awareness. Wiederholende und gut aufeinander aufgebaute Sensibilisierungsmaßnahmen der Angestellten sind der Schlüssel, um Phishing-Angreifern den Wind aus den Segeln zu nehmen. Denn ohne eine menschliche Interaktion mit den kompromittierten Mails besteht in der Regel auch keine erhöhte Gefahr – vorausgesetzt die technischen Maßnahmen des Unternehmens entsprechen einem bestimmten Sicherheitsniveau. Awareness-Schulungen sind zudem äußerst preisgünstig, vergleicht man sie mit den Wiederherstellungskosten nach einem Cyber-Angriff. Diese Art von Sensibilisierung muss jedoch regelmäßig stattfinden und sich immer an die aktuelle Sicherheitslage anpassen.



FALSCHE HINWEISE ZUR CORONA HYGIENE

Interne Phishing-Tests sollten ebenfalls essenzieller Bestandteil zur Überprüfung der Maßnahmen sein. Dabei können gefakte Phishing-Mails an die Angestellten versendet werden, um deren Reaktionen zu testen und auszuwerten. Denn Cyberkriminelle finden rasend schnell neue Wege und Möglichkeiten, um ihre Attacken zu modifizieren und an die aktuellen Umstände anzupassen. Ein gutes Beispiel für eine derartige Anpassung an aktuelle Rahmenbedingungen ist der schlagartige Anstieg solcher Mails zu Beginn der Pandemie mit Corona-Inhalten wie z.B. „Corona-Verhaltensregeln“. Diese wurden unter dem Deckmantel von Behörden und Organisationen versendet, um auf aktuelle Hygieneregelungen in der Arbeitswelt aufmerksam zu machen. Allein sie waren für zwei Prozent aller Phishing-Attacken im Februar/März 2020 verantwortlich (siehe Report European Union Agency for Cybersecurity). Der Fachbegriff für solche Attacken unter Vorwand nennt sich „E-Mail-Spoofing“. Ist die Unternehmenskommunikation transparent und sind die Beschäftigten geschult und vorgewarnt, sinkt das Risiko signifikant, dass sie solche Attacken nicht als kriminelle Handlung erkennen.

FIS-ASP Application Service Providing
und IT-Outsourcing GmbH
Röthleiner Weg 4
D-97506 Grafenrheinfeld
www.fis-asp.de