Aus dem Tagesspiegel Background Cybersecurity vom 9.2.2022

IT-Sicherheit

Von Phishing bis Vishing: Schwachstelle Mensch

Eine der größten Schwachstellen in der IT-Sicherheit ist der Mensch. Denn egal wie gut ein technisches System ist, Angreifer können häufig eine Möglichkeit finden, ihren Angriff über den Kontakt zu Personen durchzuführen. Doch es gibt Lösungsansätze.

Ulrich Hottelet

Woran hapert es bei der IT-Sicherheit? **Sandro Gaycken, Cyberkrieg-Experte und Direktor des Digital Society Institute** an der Berliner Hochschule **ESMT**, sagt im Podcast der Hochschule, er sieht als großes Problem den seit Jahren herrschenden Fachkräftemangel. Laut Gaycken gebe es „nur 40 bis 50 wirkliche Hacker in Deutschland“. Nur sie seien in der Lage, ein Unternehmen ausreichend vor Cyberangriffen zu schützen. Diese Fachkräfte würden zwischen 300.000 und 1,2 Millionen Euro jährlich verdienen. Geringer dotierte Jobs seien für sie nicht attraktiv. Mittelmäßige Talente brächten aber in der IT-Sicherheit wenig und seien eher kontraproduktiv, weil sie zum Beispiel die falsche Software kaufen oder sie falsch konfigurieren.

Ein weltweites Problem: **Marc Goodman**, Autor des Buchs „Future Crimes“ und Gayckens Gesprächspartner im Podcast der ESMT sagt: „Laut vielen Studien gibt es global etwa sechs Millionen offene Stellen in der Cybersicherheit. Fachleute in diesem Bereich erhalten auf LinkedIn zwei bis drei Anfragen pro Woche von Personalvermittler:innen. Auf Online-Jobbörsen wie Monster und Indeed werden 40 Prozent der offenen Stellen in der Cybersicherheit nicht einmal angeklickt.“

Goodman hat Organisationen wie **Interpol**, **NATO** und das **FBI** zu Cyberkriminalität und -terrorismus beraten.

95 Prozent der Datenpannen gehen auf menschliche Fehler zurück

Goodman macht im Podcast noch auf ein weiteres großes Problem aufmerksam. Er kritisiert die verbreitete Vorstellung, dass man Sicherheitsprobleme mit mehr Technologie lösen könne und zitiert dazu eine **IBM**-Studie, wonach **95 Prozent der Datenpannen auf menschliche Fehler** zurückzuführen sind. Das liegt nicht unbedingt daran, dass Mitarbeiter:innen das Thema nicht ernst nehmen, sondern daran, dass sie, zum Beispiel durch Zeitdruck, nicht immer die nötige Vorsicht walten lassen.

„70 bis 90 Prozent aller erfolgreichen Angriffe nutzen den Menschen. Das erfolgreichste Angriffsmittel ist immer noch **Phishing**“, sagt auch **Jelle Wieringa**, Security Awareness Advocate beim Trainingsanbieter **KnowBe4**. Beim Phishing geben sich Angreifer beispielsweise als vertrauenswürdige Kommunikationspartner aus, um an Daten zu gelangen oder Mitarbeiter zum Anklicken eines bösartigen Links oder Mailanhangs zu verleiten. Corona hat den Tätern das Handwerk noch erleichtert, denn im **Homeoffice sind Menschen für Phishing** anfälliger, wie eine Studie von G DATA ergab. Grund dafür ist unter anderem die schwierige Abgrenzung zwischen Arbeit und Privatem, zum Beispiel wenn die Aufmerksamkeit durch gleichzeitige Kinderbetreuung erschwert wird.

Bis zu 80 Prozent der Arbeitnehmer fallen auf den Betrug rein

Eine dieser Betrugsmaschen ist der „**CEO Fraud“**. Dabei erhalten Mitarbeiter:innen eine Nachricht, die vermeintlich aus der Führungsebene seines Unternehmens stammt. Typischerweise sollen sie dazu verleitet werden, eine Finanztransaktion vorzunehmen oder sensible Informationen preiszugeben. „Die Klickrate beläuft sich auf bis zu 80 Prozent“, sagte **Niklas Hellemann, Geschäftsführer des Trainingsanbieters SoSafe**. Zum Vergleich: Werden in der Nachricht interessante Infos, zum Beispiel vom Scanner aus der Geschäftsführung, in Aussicht gestellt, liegt die Klickrate bei 50 Prozent, immer noch ein sehr hoher Wert. **Neugier ist**

eben auch eine Erfolgsmasche beim Phishing. Ein bewährtes Gegenmittel gegen CEO-Fraud ist das Vier-Augen-Prinzip, wonach in Finanzabteilungen hohe Transaktionen vor ihrer Ausführung stets von einem zweiten Mitarbeiter geprüft werden müssen.

Doch es gibt noch viele weitere **Betrugsmaschen**, gegen die es inzwischen Lösungsansätze gibt. „Beim sogenannten **Advance-Fee-Scam** wollen die Kriminellen schnell die leichten Opfer aussortieren. Denn in einen solchen Betrug wird viel Zeit investiert. Die Angreifer gehen hier sehr wirtschaftlich vor und möchten Zeit und Ressourcen sparen“, erklärte Hellemann. Bei diesem Betrug wird dem Opfer gegen Vorab-Zahlung einer relativ kleinen Geldsumme der **Erhalt eines großen Geldbetrags** versprochen, der dann aber ausbleibt.

Wesentlich raffinierter und entsprechend schwieriger zu erkennen als die durchschnittliche Phishing-Mail ist das **Spearphishing**. Dabei wird die Zielperson zuvor zum Beispiel in sozialen Medien ausgespäht und Social Engineering eingesetzt, so dass der Nutzer eher auf die Nachricht hereinfällt und zum Beispiel den mit Schadcode versehenen Dateianhang öffnet. „Es ist ganz einfach, eine Spearphishing-Mail zu erstellen. Gegen ganz **raffinierte Spearphishing-Angriffe** hilft kaum etwas“, sagte Wieringa. Zum Beispiel könnten Täter den Namen eines Kollegen der Zielperson auskundschaften und in einer Mail an sie vorgeben, mit ihm schon über eine mögliche Kooperation gesprochen zu haben. Nähere Infos fänden sich im Mailanhang, der mit **Schadsoftware** präpariert ist.

Bedrohungslage wird sich in Zukunft noch verschärfen

In Zukunft könnte sich die **Bedrohungslage durch Künstliche Intelligenz** noch verschärfen. So fand kürzlich ein Forschungsteam von **Singapurs Government Technology Agency** in einer Studie heraus, dass KI bessere Phishing-Mails als Menschen schrieb. Denn die versuchsweise verschickten KI-generierten Spearphishing-Mails wurden häufiger geklickt als die von den Forschern erstellten. Mit KI könnten in naher Zukunft Massen von überzeugenden individualisierten Phishing-Mails erstellt werden – eine qualitativ und quantitativ neue

Herausforderung.

Eine weitere technologische Bedrohung sind **KI-basierte Deepfakes**. In der Zukunft könnten sie Voice Cloning ermöglichen, also das Imitieren der Stimmen realer Personen. Damit eröffnen sich Kriminellen neue Möglichkeiten für manipulative Telefonanrufe, sogenanntes **Voice-Phishing oder Vishing**, die dann für Mitarbeiter noch schwerer zu identifizieren sind.

Lösung liegt in der Fortbildung der Arbeitnehmer

Die Lösung, IT-Systeme nicht mehr durch den **Faktor Mensch** zu gefährden, liegt in der Fortbildung der Arbeitnehmer:innen. **Trainingsanbieter** wollen mit Schulungen Mitarbeiter:innen sensibilisieren, damit diese die **gängigen Betrugstricks** kennenlernen und dadurch nicht mehr auf sie hereinfallen. Im Anschluss erhalten sie monatlich ein bis zwei simulierte Phishing-Mails zum Test, ob sie das Gelernte auch weiterhin beherzigen. „Viele Menschen denken bei Schulungen, mit einer bestandenen Prüfung ist es getan und vergessen danach alles“, sagte Wieringa.

Durch die Test-Mails soll der Lerneffekt dauerhaft verankert werden. Mit Erfolg, so die Anbieter: Nach einem Jahr Training sinkt laut KnowBe4 die **Klickrate bei Phishing-Mails** von 38 auf vier Prozent. SoSafe berichtet, die kontinuierliche **Sensibilisierung** reduziere die Klickrate um 70 Prozent. Noch sind solche Schulungen nicht allzu weit verbreitet. Laut einem Gartner-Bericht setzen erst fünf Prozent des Mittelstands darauf.

Ein **Tipp der Anbieter** ist, dass Nutzer:innen bei ungewöhnlichen Anzeichen in einer Mail Verdacht schöpfen sollten, sei es eine Absendezeit mitten in der Nacht, eine ungewohnte Ansprache, merkwürdige Fragen eines Kollegen oder eine exe-Datei im Anhang. Im Zweifelsfall sollte man die Nachricht auf einem anderen Kanal validieren, zum Beispiel mit einem Anruf beim (angeblichen) Absender.

Ungewöhnliche Mittel im Militär

Außergewöhnlich harte Mittel, um Mitarbeiter:innen vom Ernst der Phising-Gefahr

zu überzeugen, nutzt etwa das Militär: Wie Gaycken im Podcast schildert, wird ein:e Soldat:in, der unvorsichtigerweise auf ein via Test-Mail **zugesandtes Katzenfoto** klickt, in dem sich Schadsoftware verbergen kann, von seinem vorgesetzten Offizier im Beisein seiner Kameraden eineinhalb Stunden auf dem Kasernenhof angebrüllt. Laut Gaycken soll diese Methode erfolgreich gewesen sein.

Goldman Sachs wendet eine ähnliche, aber zivilere Methode an. Beim ersten falschen Klick auf Katzenfotos muss man mit dem Chef darüber reden, beim zweiten Mal mit der **Personalabteilung** und beim dritten wird man gekündigt. Goodman nennt diese Strategie „**Cyberbestrafung“**, die in einem hierarchischen und auf Disziplin beruhenden Umfeld wie dem Militär erfolgreich ist. „Nach meiner Erfahrung funktioniert das in vielen Firmen nicht so gut, denn das entmutigt Menschen, zum Beispiel in der IT-Abteilung oder bei ihrem Chef nachzufragen, wenn sie sich unsicher sind, ob sie mit einem falschen Klick einen Fehler gemacht haben“, sagte Goodman. Er plädiert stattdessen für die „**Cyberstärkung**“ der Mitarbeiter durch deren Aufklärung über Schutzmaßnahmen.