Phishing: Wirksamer Schutz beginnt beim Mitarbeitenden

terreActive stärkt die Cyber Security am Kantonsspital Aarau mit Phishing-Simulation und Awareness-Schulung

Phishing ist eines der grössten Einfallstore für Cyberkriminelle. Ein falscher Klick auf ein gefälschtes E-Mail – die Folgen für ein Unternehmen können verheerend sein. terreActive hat beim Kantonsspital Aarau einen simulierten Angriff durchgeführt und die Mitarbeitenden mit einem Awareness-Training für die Gefahren sensibilisiert. Damit ist das Spital nun auf mögliche Attacken vorbereitet.

Wir alle kennen sie, denn sie landen fast täglich in unseren Postfächern: Spam- und Phishing-Mails, die mit gefälschten Absenderadressen, Firmenwebseiten oder vermeintlich vertrauenswürdigen Anfragen Nutzer dazu bewegen wollen, sensible Informationen preiszugeben oder Schadsoftware zu installieren. In der Regel verraten sich die Versender der Betrugsnachrichten durch Rechtschreibfehler, unspezifische Ansprache oder andere Ungereimtheiten. Doch die Phishing-Angriffe werden immer raffinierter und ihre Erfolgsquote steigt.

Es sind die personalisierten, auf die Empfänger zugeschnittenen Phishing-Nachrichten, die für Unternehmen ein hohes Risiko darstellen können. Oftmals sind sie das Einfallstor für Hackerangriffe, die schwerwiegende Folgen haben können, wie etwa Ransomware, die Daten, Verzeichnisse oder gar die gesamte Festplatte verschlüsselt und der Hacker für die Entschlüsselung ein Lösegeld fordert. Dies zeigen verschiedene Fälle, bei denen es Angreifern gelang, Teile der IT-Infrastruktur oder ganze Betriebe lahmzulegen. Das Kantonsspital Aarau (KSA) suchte nach einer Lösung, um sich vor solchen Attacken besser zu schützen. Es fand sie beim Security-Spezialisten terreActive.

Security-Bewusstsein auf die Probe stellen

Das KSA ist mit über 30 Behandlungs- und Diagnosezentren sowie rund 4600 Angestellten und über 28'000 stationären Patientinnen und Patienten das grösste Spital im Kanton Aargau.

«In der Vergangenheit war das Thema Security-Bewusstsein bei Mitarbeitenden nicht im Detail adressiert worden. So war es ein richtiger und wichtiger Entscheid der Sicherheitsverantwortlichen des KSA, diese Problematik anzugehen,» sagt Martin Matter, CTO des KSA.

Gegen Phishing-Attacken hat sich ein Paket aus verschiedenen Massnahmen bewährt:

- Es braucht eine Anti-Phishing-Strategie, hinter der die ganze Organisation steht.
- Es braucht die richtigen Hilfsmittel, z. B. eine Lösung mit der man Angriffe simulieren kann, um anschliessend eine erste Risikobewertung zu erstellen.
- Zudem braucht es Awareness-Schulungen für die Sensibilisierung aller Mitarbeitenden.

Für die Unterstützung bei diesen Massnahmen, wandte sich das KSA an terreActive. Mit seinen mehr als 20 Jahren Erfahrung in der Cybersecurity war das Unternehmen der perfekte Partner für diese Aufgabe. terreActive führte für das KSA eine Phishing-Simulation und ein Awareness-Training durch. Dabei wird zuerst eine Phishing-Attacke auf das Unternehmen simuliert, um den aktuellen Stand der Gefährdung sowie den Grad der bereits vorhandenen Sensibilisierung der Mitarbeitenden in Erfahrung zu bringen.

Tools im Einsatz:
LUCY Security made in Switzerland

Die Social-Engineering-Plattform von LUCY Security bietet eine grosse Auswahl an Funktionen, Phishing-Simulationen, Awareness-Trainings, Reports sowie weitere Services an. Die Plattform wird regelmässig weiterentwickelt, um mit den raffinierten Methoden der Hacker Schritt zu halten. terreActive verfügt als offizieller Partner von LUCY über mehrere Jahre Erfahrung mit der Plattform. www.lucysecurity.com/de

Ablauf des Phishing-Projekts

Der erste Schritt des Phishing-Projekts bestand darin, in einem Kick-off-Meeting mögliche Angriffs-Szenarien und Awareness-Botschaften festzulegen. Nach den technischen Vorbereitungen und einer finalen Freigabe durch das KSA schickten die Security-Experten von terreActive ein fingiertes Mail an die Mitarbeitenden des KSA. Das Phishing-Mail war auf die Gegebenheiten im Spital zugeschnitten, enthielt aber auch auffällige Fehler, einen unbekannten Absender und andere Abweichungen von den am KSA üblicherweise verschickten Nachrichten. Trotz dieser Warnhinweise klickt ein grosser Teil der angeschriebenen Mitarbeitenden auf den Phishing-Link im Mail. Sehr viele davon gaben ihre Zugangsdaten auf der Phishing-Website ein, die sich hinter dem Link verbarg. «Unsere Mitarbeitenden erlebten so unmittelbar, mit welchen Methoden ein potenzieller Angreifer an Informationen kommen kann» so Martin Matter. Aus langjähriger Social-Engineering-Erfahrung weiss terreActive, dass sich die Ergebnisse des KSA durchaus in der Norm bewegten, heisst, dass leider auch bei anderen Unternehmen – *vor* einer Awareness-Schulung – zu viele Mitarbeitende auf die fingierten Mails hereinfielen.

Gefahr erkannt – Gefahr gebannt

Auf den Mailversand folgte der zweite Teil des Projekts: eine Awareness-Kampagne. Die Mitarbeitenden des KSA wurden über Risiken und richtiges Verhalten beim Empfang unbekannter oder verdächtiger Mails aufgeklärt. Zusätzlich wurde für alle Angestellten ein webbasierter Kurs zusammengestellt, um ihren Wissensstand abzufragen, Schwachstellen zu thematisieren und sie bei der Erkennung von Phishing zu unterstützen. terreActive wertete die Resultate sowohl des Phishing-Tests wie auch der Awareness-Schulung zuhanden der Geschäftsleitung des KSA aus und erstellte einen umfangreichen Abschlussbericht mit Statistiken, einer ausführlichen Analyse, technischen Schwachstellen und Massnahmenempfehlungen.

Allen Mitarbeitenden des KSA, die sich an der Schulung beteiligten, gilt ein besonderer Dank, denn beides fand im Frühjahr 2020 statt, also unter der speziellen Belastung der ersten Covid-Welle.

Über das Kantonsspital Aarau

Das Kantonsspital Aarau (KSA) ist neben den Universitätsspitälern eines der grössten Zentrumsspitäler der Schweiz. Das Leistungsangebot reicht von der Grundversorgung bis hin zur hochspezialisierten Medizin. Es gibt rege Forschungstätigkeit und ein umfassendes Weiterbildungsangebot für Fachpersonal.

In über 30 Behandlungs- und Diagnosezentren zeichnen rund 4600 Fachpersonen aus Diagnostik, Medizin, Pflege, Therapie und anderen Berufsbereichen jährlich für fast 28'000 stationäre und über 520'000 ambulante Behandlungen verantwortlich.
www.ksa.ch

Kantonsspital Aarau

Mails mit unbekanntem Absender, verdächtig wirkendem Betreff oder ungewöhnlichem Anhang: Das Problem Phishing ist bekannt, trotzdem gibt es immer wieder betroffene Unternehmen und der Schaden ist beträchtlich. Kontrollierte Angriffe und präventive Awareness-Schulungen wie jene beim KSA vermindern einen Ernstfall mit Umsatzausfall, Kosten für den Ersatz von IT-Infrastruktur und Imageschaden.

Eine wirksame Anti-Phishing-Strategie steht und fällt dabei mit dem Bewusstsein der Mitarbeitenden. So einfach diese Erkenntnis ist, so gross sind aber auch die Hürden, dieses Bewusstsein zu schaffen – trotz erschreckend hoher Trefferquote im Test. Das Thema interessiert viele der Anwender nicht, weiss CTO Martin Matter auch aus Gesprächen mit anderen Spitälern. Die Bereitschaft dazuzulernen, ist äusserst bescheiden. Technische Massnahmen alleine reichen nicht aus, um einen Angriff von Cyberkriminellen abzuwehren. Es braucht dazu ein orchestriertes Zusammenspiel von Führung, Technik und Mitarbeitenden. Etwa durch regelmässige Phishing-Simulationen sowie Sensibilisierungsmassnahmen, wie terreActive sie für das KSA durchführen durfte.