schleupen

Effizienz, die verbindet.

FACHBEITRAG ZUR IT-SICHERHEIT

Wenn der Faktor Mensch zum Sicherheitsrisiko wird.

Mit SoSafe Awareness-Training den Schutz vor Phishing-Attacken stärken.

IT-Sicherheit

Wenn es um den Schutz vor Cyberattacken geht, denken die meisten Menschen zuerst an technische Lösungen, wie zum Beispiel Virenscanner oder das Schließen von Sicherheitslücken in Anwendungen. Dabei ist es oft der Klick eines Mitarbeitenden auf eine präparierte E-Mail, der Hackern die Tore öffnet. Geschulte, aufmerksame Mitarbeitende sind deshalb ein wichtiges Glied in der IT-Sicherheitskette eines Unternehmens.

Die besten Firewalls und Virenscanner sind machtlos, wenn ein Hacker das Passwort von einem Mitarbeitenden einfach mitgeteilt bekommt. Es klingt unwahrscheinlich, dass so etwas passiert? Es passiert viel häufiger, als viele denken. Eigentlich ist es die ganz normale Realität. Dabei handeln die Beschäftigten im Unternehmen meist ohne Vorsatz, sondern fallen auf raffinierte, betrügerische E-Mails, sogenannte Phishing-Mails, herein. Über 92 Prozent aller Cyberangriffe starten mit solch einer betrügerischen Mail. Eine von drei Phishing-Mails wird angeklickt. Nach Erkenntnissen des Virenexperten McAfee passieren von täglich 156 Millionen Phishing-Mails immerhin 16 Millionen die Spamfilter der Mailprogramme. Dazu kommt: 72 Prozent aller Anwender verwenden das gleiche Passwort mehrfach. Es ist also wahrscheinlich, dass gleich mehrere Türen geöffnet werden, wenn das Passwort erst einmal bekannt ist.

KLEINE MENSCHLICHE SCHWÄCHEN

Das sind erschreckende Zahlen, die zeigen, dass Spamfilter und Appelle an die Aufmerksamkeit allein anscheinend nicht ausreichen, um die Gefahr durch Phishing und Social Engineering* zu bannen. Insbesondere die Energie- und Wasserwirtschaft, die als Teil der sogenannten Kritischen Infrastruktur (Kritis) im Fokus von Cyberattacken steht, ist zu besonderer Wachsamkeit aufgerufen. Denn die Methoden der Hacker werden immer raffinierter und machen sich kleine menschliche Schwächen gezielt zunutze. Dazu gehören Neugier, Unaufmerksamkeit, Gutgläubigkeit oder auch unreflektierter Respekt gegenüber einem Vorgesetzten.

GEFÄLSCHTE MAILS WIRKEN ECHT

Immer öfter sind Phishing-Mails keine plumpen Täuschungsversuche, sondern verblüffend echt wirkende E-Mails. Dabei nutzen Hacker jede Menge Informationen, die sie über ein Unternehmen und seine Mitarbeiter finden. Als geschickte Rechercheure durchforsten sie Homepage, Zeitungsberichte und Social-Media-Profile. Es ist erstaunlich, wie oft sich aus diesen öffentlich zugänglichen Daten ein präzises Bild zeichnen lässt. Das gibt Hackern die Chance, sich sehr glaubwürdig als jemand anderes auszugeben.

Es braucht schon Geistesgegenwart und Expertise, um die kleinen Abweichungen in einer gefälschten Mail zu entdecken, die sich häufig in der Absenderadresse finden und verraten, dass die Mail von einer anderen Domäne versandt wurde. Oftmals hilft nicht einmal das, wenn die Hacker den Mail-Account eines Korrespondenzpartners gekapert haben. Von hier aus können sie Mails schicken, die an aktuelle Gesprächssituationen anknüpfen und über den „richtigen" Absender verfügen. Wer dieser Gefahr wirkungsvoll begegnen will, braucht nicht nur einen Sicherheitsexperten im Unternehmen, sondern muss alle Mitarbeitenden zu Sicherheitsexperten machen.

AUFMERKSAMKEIT ZUR ROUTINE MACHEN

Um die Wachsamkeit von Mitarbeitenden gezielt zu trainieren, hat der Sicherheitsanbieter SoSafe ein spezielles Trainingsprogramm entwickelt, das als SaaS-Lösung angeboten wird. Es besteht aus einem E-Learning-Modul und einem Modul, das Phishing-Attacken simuliert, sowie einer Reihe von Tracking- und Analyse-Tools. Da die Schleupen AG als Softwareentwickler für Unternehmen der Kritis selbst im Fokus der Hacker steht, hat sie die Lösung ihres Partners SoSafe selbst seit einigen Jahren im Einsatz.

Das E-Learning-Modul umfasst dabei alle relevanten Themen, um Mitarbeiter fit zu machen im Umgang mit Cyberbedrohungen. In einzelnen, handlichen Lektionen lernen sie dabei, welche Strategien Angreifer verfolgen, wie sie sich bei Sicherheitsvorfällen verhalten sollen oder was sie beim Thema Passwörter beachten müssen.

* *Social Engineering* bezeichnet den Versuch, Personen so zu beeinflussen, dass sie sich in bestimmter Weise verhalten, bspw. vertrauliche Informationen preisgeben. Dazu wird oft das persönliche Umfeld des Opfers ausgespäht. So können glaubwürdig vorgetäuschte Identitäten aufgebaut werden.

DEN ERNSTFALL PROBEN

Der eigentliche Clou der SoSafe-Lösung sind simulierte Angriffe, die exakt auf die jeweilige Branche zugeschnitten sind. So gibt es eine spezielle, direkt auf die Unternehmen der Energie- und Wasserwirtschaft zugeschnittene Version, die von Schleupen angeboten wird. In dem Paket enthalten ist beispielsweise die Beschwerde eines verärgerten Kunden über eine fehlerhafte Rechnung oder die angebliche Warnung bzgl. einer Grenzwertüberschreitung im Trinkwasser – alles Themen, die auch im echten Geschäftsbetrieb aufkommen. Bei SoSafe können sogar individualisierte Mails gebucht werden, die auf die spezielle Situation im Unternehmen des Anwenders Bezug nehmen. Dadurch wirken die Mails täuschend echt. Klickt ein Mitarbeiter auf einen Link in der fingierten Mail, öffnet sich ein Fenster. Hier wird er über die Gefahren aufklärt, die gedroht hätten, wenn der Angriff echt gewesen wäre.

Durch dieses Verfahren erleben die Mitarbeitenden am eigenen Leib, wie leicht sie hinters Licht zu führen sind. Außerdem sorgt die ständige Gefahr, auf eine simulierte Mail hereinzufallen, für erhöhte Aufmerksamkeit. Mit der Zeit achten sie immer mehr auf die kleinen Anzeichen, die auf eine Fälschung hinweisen. Im Zuge des Programms verringern sich die Klickraten deshalb nachweislich. Denn erst die Kombination aus Wissen und Aufmerksamkeit sorgt für das Maß an Sicherheit, das in Unternehmen der Kritischen Infrastruktur nötig ist. Der Branchenfokus macht es auch kleineren Stadtwerken, die sonst keine Kapazitäten dafür hätten, möglich, den Mitarbeitenden ein maßgeschneidertes Training anzubieten.

Im Backend des Systems kann der Administrator verfolgen, wie groß die Gefahren sind und ob seine Kollegen Fortschritte machen. Im Zweifelsfall kann er mit gezielten Schulungsmaßnahmen gegensteuern.

Dr. Peter Wenderoth, Assistent der Geschäftsleitung und bei der Schleupen AG zuständig für Datensicherheit und Datenschutz, zieht nach zwei Jahren SoSafe im Unternehmen eine positive Bilanz: „Auch wir als Softwarehersteller sehen immer wieder selbst, dass Sicherheit dauernd und von allen geübt werden muss. Deshalb ist SoSafe eine wesentliche Säule unseres Sicherheitskonzepts. Denn das Gesamtkonzept ist immer nur so gut wie sein schwächstes Glied. Und das schwächste Glied ist leider häufig der Mensch."

Sprechen Sie uns an, wenn Sie mehr zu diesem Thema erfahren möchten.

Schleupen SE
Galmesweg 58
47445 Moers

Tel.: 02841 912-0
E-Mail: vertrieb@schleupen.de