Beitrag auf medinside.ch, dem Portal für die Gesundheitsbranche,
vom 5. Februar 2020

Cyberattacken: Mehr Mensch als Technik

Cyberattacken stellen eine grosse Gefahr für das Gesundheitswesen dar. Oft geraten dabei die Mitarbeitenden in das Fadenkreuz der Cyberkriminellen. Die Lösung ist ein ganzheitlicher Ansatz aus technischen Abwehrmassnahmen, dem Einsatz von Spezialisten und der Sensibilisierung der Mitarbeitenden.

Die Digitalisierung schreitet mit grossen Schritten voran, dabei werden auch die kritischen Stimmen lauter. Neben den Herausforderungen drängen sich auch die Risiken immer mehr in den Vordergrund. Eine offensichtliche und unbestreitbare Gefahr sind Cyberattacken. Im Gesundheitswesen kann es da rasch um Leben und Tod gehen. Folglich gewinnt die IT-Sicherheit an Bedeutung. Die Erforschung der Rolle des Menschen in der IT-Sicherheit befindet sich noch in den Anfängen. Bereits heute ist klar: Das Mitwirken der Mitarbeitenden ist entscheidend für die Robustheit eines Unternehmens gegen Cyberattacken. Dies zeigt eine Analyse der häufigsten Angriffsszenarien.

Ein Phish im Netz genügt

Der Grossteil der Cyberattacken erfolgt mittels Spam-E-Mails. Empfänger werden auf gefälschte und schadhafte Websites gelockt oder dazu verleitet, mit Malware, also schädlicher Software wie Viren und Trojaner, infizierte E-Mail-Anhänge zu öffnen. Diese sogenannten Phishing-Attacken (Phishing von engl. password harvesting, Passwörter sammeln, und fishing, Angeln) stellen eine grosse Gefahr für Organisationen dar. Zum einen können Cyberkriminelle Zugriff auf sensitive Informationen erlangen. Zum anderen kann Malware das Computersystem einer Organisation infizieren und dieses letzten Endes lahmlegen. Wie aktuelle Beispiele zeigen, kann dies im Falle eines Spitals gravierende Folgen haben, etwa wenn dieses Patienten abweisen muss.

Da das Versenden verhältnismässig einfach und günstig ist, übersteigt die Anzahl von Spam-E-Mails die der sauberen E-Mails bei weitem. Die Taktik der Cyberkriminellen ist offensichtlich: Durch die massenhafte Versendung erhöht sich die Wahrscheinlichkeit, dass Spam-E-Mails zu den Empfängern gelangen. Einmal empfangen, liegt es an den Empfängern, ob diese die E-Mail als Phishing-Versuch erkennen oder den Cyberkriminellen ins Netz gehen.

Man muss davon ausgehen, dass jede Organisation und Person in der Schweiz bereits solche unerwünschten E-Mails erhalten hat, diese aber meistens durch Spam-Filter blockiert werden. Daher geben nur etwas mehr als die Hälfte aller KMU in der Schweiz an, von Spam-Mails betroffen zu sein. Spam-Filter funktionieren also gut.

Der Grossteil der Phishing-Attacken wird verhindert, und nur wenige Spam-E-Mails erreichen die Empfänger. Zugestellte Spam-E-Mails werden häufig von den Empfängern als solche wahrgenommen, es ist aber unmöglich, jede Spam-E-Mail herauszufiltern und als solche zu erkennen. Derweil genügt eine einzige erfolgreiche Phishing-Attacke, um einer Organisation nachhaltig zu schaden. Und so sind mehr als ein Drittel aller KMU in der Schweiz von Viren und Trojanern betroffen.

Technische Abwehrmassnahmen wie Virenschutz und Firewall sind notwendig, aber unzureichend, um ein Computersystem vor Viren und Trojanern zu schützen. Wenn Nutzer Malware aktiv installieren, umgehen sie unbeabsichtigt die technischen Abwehrmassnahmen und werden so zum Einbruchswerkzeug der Cyberkriminellen. Technische Abwehrmassnahmen sind also nur so stark, wie der Mensch es zulässt.

Täuschung schlägt Mensch und Technik

Auf die Frage, wieso genau Phishing-Attacken erfolgreich sind, gibt es keine abschliessende Antwort. Vermessen wäre es, den Opfern erfolgreicher Attacken die Schuld zu geben. Phishing-Attacken sind kriminelle Handlungen und Cyberkriminelle sind die Täter. Einige Forschende haben sich mit den Phishing-Methoden genauer auseinandergesetzt. Es zeigt sich, dass Methoden zum Einsatz kommen, welche die Empfänger teils sehr raffiniert täuschen. Diese werden mit dem Begriff Social Engineering zusammengefasst. Social Engineering nutzt zum einen den sozialen Kontext aus, zum anderen aber auch gezielt die individuelle Situation der Empfänger.

Dabei ist der meist genutzte Ansatz in Phishing-Attacken das Vorgeben von Autorität. So neigt der Mensch dazu, Aufforderungen von Autoritätspersonen nachzukommen. Zum einen erwartet die Gesellschaft von ihren Mitgliedern, Autoritäten zu achten. Zum anderen orientieren Menschen sich in unklaren und stressvollen Situationen gern an Autoritäten. Wenn also in einer Spam-E-Mail vorgegeben wird, dass diese von einem Vorgesetzten kommt, steigt die Wahrscheinlichkeit, dass der Empfänger auch einer zweifelhaften Anfrage nachkommt – vorausgesetzt die E-Mail wird als authentisch wahrgenommen.

> «Bedrängnis und Zeitdruck lassen Menschen spontane, unüberlegte Entscheidungen treffen.»

Geradezu heimtückisch sind Phishing-Attacken, in denen die Versender vorgeben, System-Administratoren zu sein und vom Empfänger verlangen, ein notwendiges Sicherheitsupdate zu installieren. Insbesondere Organisationen mit starken Hierarchiestrukturen sind hierbei gefährdet. Ergänzend hierzu können auch auf andere Weisen das vermeintlich gesellschaftlich konforme Verhalten eingefordert oder die Empfänger in Bedrängnis und unter Zeitdruck gebracht werden. So lassen Bedrängnis und Zeitdruck Menschen spontane, unüberlegte Entscheidungen treffen. Wenn beispielsweise eine Person am Freitagnachmittag einen medizinischen Notfall, wie das Ausgehen eines Medikaments vorgibt und per E-Mail dringend um Verlängerung des Rezepts bittet, wird dabei die korrekte Authentifizierung der Person möglicherweise vergessen.

Neben diesen vorgetäuschten Situationen kann auch die alltägliche Leistungserwartung bei der Arbeit dazu führen, dass Mitarbeitende auf Phishing-Attacken hereinfallen. Der Fokus liegt auf der Erfüllung der Aufgabe, und E-Mails werden häufig automatisiert, ohne nachzudenken geöffnet, dazu sind Arbeitskollegen nebenan möglicherweise laut am Telefonieren. Dies sind alltägliche Situationen, die unsere Aufmerksamkeit unbewusst

steuern und somit für Ablenkung sorgen. Dabei muss man sich in Erinnerung rufen, dass Phishing-Attacken kriminelle Taten sind, die aktiv täuschen und manipulieren. Oft wirken Spam-E-Mails täuschend echt, sind optisch und inhaltlich kaum bis gar nicht als Fälschung zu erkennen.

> «Cyberattacken in Form von Phishing basieren auf der menschlichen Interaktion, entsprechend sollten die Mitarbeitenden hierfür regelmässig geschult werden.»

Sensibilisierung der Anwender

Die Herausforderung besteht darin, diese Gefahr möglichst zu minimieren. Aber wie genau ist dies möglich? Als Lösungsansatz hat sich die Security Awareness, also die Sensibilisierung der Mitarbeitenden für sicherheitsbewusstes Verhalten bewährt. Dabei spielt technisches Wissen eine untergeordnete Rolle. Cyberattacken in Form von Phishing basieren auf der menschlichen Interaktion, entsprechend sollten die Mitarbeitenden hierfür regelmässig geschult werden.

Mitarbeitende müssen branchenspezifisch und praxisnah auf mögliche Gefahren und Szenarien vorbereitet werden. Dabei ist Security Awareness kein Projekt mit einmaligen Massnahmen. Die Mitarbeitenden werden bei diesem Ansatz fortlaufend auf ihre eigene Verwundbarkeit aufmerksam gemacht, kennen die aktuellen Gefahren und potentiellen Auswirkungen. Dabei sollten sich die Mitarbeitenden den IT-Sicherheits-Verhaltensregeln bewusst sein, in der Lage sein diese einzuhalten und wissen wann die Unterstützung durch Spezialisten angebracht ist.

Autor: Jona Karg

Jona Karg studiert an der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW) angewandte Psychologie. In mehreren wissenschaftlichen Arbeiten erforscht er die Rolle des Menschen in der IT-Sicherheit. Bei der Health Info Net AG (HIN) ist er für die Weiterentwicklung der Awareness Schulungen sowie des Awareness E-Learnings verantwortlich.