Steigendes Interesse an Audits, Awareness-Trainings und Penetrationstests durch starke Zunahme von Social Engineering-Attacken

100% Erfolgsquote: Jedes secion IT-Security Audit legt Schwachstellen offen

Hamburg, 02. Mai 2018 – Der Hamburger IT-Sicherheitsspezialist secion verzeichnet stark steigende Nachfragen im Bereich der IT-Security Audits. Vor allem der Anteil an Awareness-Trainings zum Schutz vor Social Engineering-Attacken ist 2017 im Vergleich zum Vorjahr um mehr als das Zehnfache gestiegen. Den Grund für den starken Anstieg sieht secion vor allem in der hohen Erfolgsquote, die Cyberkriminelle mittlerweile durch verschiedenste Angriffsformen für sich verbuchen können. Den Penetrationstestern von secion ist es bisher in jedem dieser Audits gelungen, Schwachstellen aufzudecken. Durch konkrete Handlungsempfehlungen zur Schließung der IT-Sicherheitslücken sowie Awareness-Schulungen für Mitarbeiter konnte die IT-Sicherheit der Unternehmen durch secion maßgeblich gesteigert werden.

Social Engineering bezeichnet die Manipulation durch Betrüger, die sich das Vertrauen anderer Menschen erschleichen, um bestimmte Verhaltensweisen auszulösen. In der Cyberkriminalität werden diese Angriffsmuster verwendet, um Angestellte zur Herausgabe geheimer Informationen, Passwörter, unbezahlter Dienstleistungen oder sogar Geld zu bewegen. Auch Phishing-Attacken, die das Ziel haben, Zugangsdaten zu Unternehmenskonten zu erlangen, zählen zu dieser Form der Manipulation. Durch die Medien bekannt geworden sind zum Beispiel die sogenannten „CEO-Frauds“. Kriminelle spionieren dabei Verhaltensweisen von Vorgesetzten und Untergebenen aus. Mit einer gefälschten E-Mail geben diese Kriminellen dann beispielsweise als Vorgesetzter Handlungsanweisungen wie die Überweisung von Geldbeträgen. Bei dieser Form von Angriffen sind technische Maßnahmen allein wirkungslos, denn die Angriffe zielen nicht auf die IT-Infrastruktur eines Unternehmens, sondern auf die Mitarbeiter.

Mitarbeiter schulen – Social Engineering verhindern

Um sich vor solchen Angriffen zu schützen, ist es erforderlich, die Angriffsmechanismen zu kennen. Dafür nutzt secion eine Reihe von Penetrationstests und weitere IT-Security Audits mit unterschiedlichen Schwerpunkten. „Besonders stark werden in letzter Zeit Social Engineering Audits bei uns angefragt“, sagt Patrick Jung, Leiter Professional Services bei secion. „Dabei nutzen unsere Penetrationstester die gleichen Strategien, die auch Cyberkriminelle bei einer echten Social Engineering-Attacke nutzen würden.“

Elementarer Bestandteil des Social Engineering-Audits ist stets eine Erörterung der Überprüfungsergebnisse. Häufig werden von den auftraggebenden Unternehmen im Anschluss an ein Social Engineering Audit Awareness-Schulungen für ihre Mitarbeiter beauftragt, um deren Sicherheitsbewusstsein zu sensibilisieren bzw. optimieren. Diese Schulungen lassen sich über den secion Awareness-Konfigurator online zusammenstellen und auf die individuellen Bedürfnisse der Unternehmen zuschneiden.

Bei den technischen Audits liegen in der Kundennachfrage die White Box Audits im Fokus der Kundennachfrage. Vor dem Test werden den verantwortlichen Penetrationstestern alle notwendigen Informationen über IT-Systeme und interne Unternehmensstrukturen zur Verfügung gestellt. Sind diese Informationen nicht verfügbar, handelt es sich um ein Black Box Audit.

Zunehmende Gefahr aus den eigenen Reihen: Der Innentäter

Bei Innentäter-Audits verzeichnete secion von 2016 bis 2017 sogar eine Steigerung der Nachfrage um das Vierfache. Diese IT-Security Audits behandeln die Gefahr von Innentätern. Das sind Mitarbeiter oder Partner, die besonders leicht an sensible Daten gelangen und sich diese zunutze zu machen können. Ihre Zugangsmöglichkeiten und Kenntnisse über innerbetriebliche Abläufe machen Innentäter für Unternehmen besonders gefährlich, und ein Innentäterangriff kann erheblichen finanziellen Schaden verursachen. Die auf Innentäter spezialisierten IT-Security-Audits nehmen technischen Normen sowie Prozessrichtlinien unter die Lupe und prüfen beispielsweise, ob die eine unzulässige Erhöhung der Rechte eines Innentäters auffällt.

Jedes Unternehmen ist angreifbar

„Bisher konnten wir bei jedem der von uns durchgeführten IT-Security-Audits Schwachstellen aufdecken – und sind damit glücklicherweise realen Angreifern zuvorgekommen.“, fasst Patrick Jung den Erfolg der Methoden von secion zusammen. „Nach einem Penetrationstest sprechen wir konkrete Handlungsempfehlungen aus. So unterstützen wir die Unternehmen dabei, ihre IT-Sicherheitslücken zu schließen. Selbstverständlich bieten wir auch Re-Audits an, die aufzeigen, ob die aufgedeckten Schwachstellen erfolgreich geschlossen wurden.“

Weitere Informationen finden Sie unter www.secion.de.

Über die secion GmbH:
Gegründet im Jahr 2004, hat sich die secion GmbH als führender Spezialist für IT-Sicherheit in Deutschland etabliert. Das Unternehmen mit Sitz in Hamburg ist insbesondere auf Lösungen und Consulting in den Bereichen E-Mail-Security, Data Leakage Prevention, Network Security, Gateway und Endpoint Protection spezialisiert. Zudem engagiert sich secion für die Sensibilisierung in puncto IT-Sicherheit und bietet Unternehmen individuelle Security Workshops, Security Audits sowie Penetrationstests an. Awareness-Schulungen vermitteln Anwendern essenzielles Wissen und das Bewusstsein für IT-Sicherheit. Um ihre Erfahrungen mit den deutschen Unternehmen zu teilen, ist secion Partner der Allianz für Cyber-Sicherheit, einer Initiative des Bundesamts für Sicherheit in der Informationstechnik (BSI). Über dieses Engagement gibt secion Erfahrungswerte und IT-Sicherheitsanalysen den Partnern und Teilnehmern der Allianz aus der deutschen Wirtschaft bekannt. Mehr Informationen unter www.secion.de.

Weitere Informationen:

secion GmbH
Paul-Dessau-Str. 8
D-22761 Hamburg
Telefon: 040/38 90 71-0
Fax: 040/38 90 71-299
www.secion.de

Ansprechpartner:
Marcus Henschel
Geschäftsführer
Tel.: 040/38 90 71-0
E-Mail: mh@secion.de

Kommunikationsagentur:
Sprengel & Partner GmbH
Nisterstraße 3
D-56472 Nisterau
www.sprengel-pr.com

Ansprechpartner:
Samira Liebscher
Marketing Consultant
Tel.: +49 (0)26/61-91 26 0-0
E-Mail: sl@sprengel-pr.com