secion optimiert Abwehrmaßnahmen in Unternehmen

Red Team Testing: Hackerangriffe für die IT-Sicherheit

Hamburg, 09. Januar 2018 – Der Hamburger IT-Sicherheitsspezialist secion bietet mit dem Red Team Testing die nächste Entwicklungsstufe des Penetrationstests an. Dabei werden die Abwehrfähigkeiten von Unternehmen unter realen Bedingungen getestet. Das Angebot richtet sich vor allem an Groß- und Mittelstandsunternehmen sowie Konzerne. Zur Zielgruppe gehören außerdem Banken und Behörden, die besondere Gefahr laufen, Opfer von Wirtschaftsspionage und organisierter Kriminalität zu werden. Für das Angebot besteht Bedarf, so konnte zum Beispiel die Hackergruppe MoneyTaker[1] mit einer Serie von Cyberangriffen seit 2016 mehr als 10 Millionen US-Dollar von über zwanzig Banken stehlen.

Red Team geht wie bei einem echten Cyberangriff vor und testet die Abwehr- und Reaktionsfähigkeit eines Unternehmens. Dabei werden reale Gefahren für die kritischen Vermögenswerte und Kernprozesse einer Organisation durch Cyberkriminalität aufgedeckt und mögliche Abwehrmaßnahmen gegen echte Eindringlinge getestet und trainiert. Laut dem Mandiant M-Trends Report 2017[2] dauert es durchschnittlich 99 Tage, bis Unternehmen einen Angriff überhaupt erkennen. In dieser Zeitspanne kann der Angreifer erhebliche Schäden verursachen. Trotz dieser erschreckenden Zahl unterschätzen viele Unternehmen die Gefahr durch Hackerangriffe sowie die daraus resultierenden Folgen. Die Angriffssimulation des Red Team trainiert das firmeninterne IT-Team und schafft ein Bewusstsein für mögliche Handlungen oder Taktiken der Angreifer.

Hackerangriff für die Unternehmenssicherheit

Die IT-Sicherheitsexperten des secion Red Team handeln als „freie Angreifer“ und unterliegen keinerlei Einschränkungen. Die Taktiken und eingesetzten Mittel entsprechen dabei denen eines realen Angreifers, der die kritischen IT-Infrastrukturen infiltriert, um sich nach und nach mehr Rechte im System zu erschleichen und so, wie beispielsweise im Fall der Hackergruppe MoneyTaker, sensible Daten zu manipulieren. Bei der umfassenden Angriffssimulation bezieht das Red Team die gesamte Umgebung eines

[1] Quelle: https://www.heise.de/newsticker/meldung/Hackergruppe-MoneyTaker-erbeutet-10-Millionen-US-Dollar-von-ueber-zwanzig-Banken-3916118.html.
[2] Mandiant M-Trends 2017: http://files.shareholder.com/downloads/AMDA-254Q5F/0x0x938351/665BA6A3-9573-486C-B96F-80FA35759E8C/FEYE_rpt-mtrends-2017_FINAL2.pdf.

Unternehmens mit ein. Dabei versucht es, über einen möglichst langen Zeitraum handlungsfähig zu bleiben, um Risiken, potentielle Gefahren und Folgeschäden eines realen Angriffs zu verdeutlichen.

Angreifer erfolgreich abwehren

Nach der Infiltrationsphase wird die IT-Abteilung des Unternehmens kontaktiert und erhält durch die Security Consultants des Red Team Informationen zu ihrer Vorgehensweise und Angriffstaktik. Dadurch findet ein entscheidender Lerneffekt statt, so dass beim nächsten Angriffsversuch die Beantwortung beispielweise folgender Fragen zeitnah erfolgen kann: Wie erkennt man, dass die IT infiltriert wurde? Wie kann man den Angreifer im eigenen Netzwerk schnellstmöglich handlungsunfähig machen? Ziel des Verfahrens der wiederkehrenden Angriffssimulation ist es, Angriffe schneller zu erkennen (Time To Detection reduzieren) und die Zeitspanne bis zum Erreichen des nächsten Szenarioziels durch das Red Team zu verlängern (Time To Adversary Success verlängern).

„Angriffe sind heutzutage komplex und heimtückisch. Zudem stellen wir uns längst nicht mehr die Frage, ob es zu einem Angriff kommen wird. Die Frage lautet längst, wie schnell der Angriff erfolgreich sein wird. Dadurch ist es für Sicherheitsverantwortliche von Unternehmen wichtiger denn je, die Taktiken von Angreifern und deren eingesetzte Mittel und Wege für ihre Zielerreichung zu verstehen und wirksame Gegenmaßnahmen zu kennen“, sagt Patrick Jung, Leiter Professional Services bei secion. „Dieses Wissen ist entscheidend für die Informationssicherheit jedes Unternehmens. Mit dem secion Red Team setzen wir neue Maßstäbe und optimieren die Angriffsabwehr von Organisationen, damit diese dem realen Angreifer einen entscheidenden Schritt voraus sind.“

Weitere Informationen finden Sie 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