KEINE CHANCE FÜR HACKER: SVA SORGT MIT EINEM PENETRATION TEST FÜR MEHR SICHERHEIT BEI SER GROUP

„Für uns war ein externer Penetration Test ein wichtiges Instrument, um unsere Netze im Hinblick auf Datenschutz und Business Continuity zu untersuchen.“

„Wir haben uns für SVA entschieden, weil wir mit dem Dienstleister schon längere Zeit ein vertrauensvolles Verhältnis in Bezug auf unsere Sicherheitssysteme haben.“

DIE HERAUSFORDERUNG

Cyber-Kriminelle benötigen oft nur wenige Minuten, um in ein IT-System eines Unternehmens einzudringen und an wertvolle Informationen und Daten zu gelangen. Dabei werden die Angriffe häufig erst nach Wochen oder Monaten bemerkt. In der Zwischenzeit können die Hacker in aller Ruhe ihr Unwesen treiben. Ein regelmäßiger Penetration Test, auch Pentest genannt, beugt solchen Angriffen frühzeitig vor. Er simuliert einen Angriff und deckt Sicherheitslücken auf, sodass diese rechtzeitig geschlossen werden können. Gleichzeitig hilft ein Pentest, nachzuweisen, dass die operativen IT-Risiken wirksam gemanagt werden. Besonders wichtig ist dies zum Beispiel vor dem Hintergrund der EU-DSGVO oder einer angestrebten Zertifizierung nach ISO 27001 oder BSI Grundschutz.

Die meisten Hacks passieren, weil Schwachstellen über Jahre unentdeckt bleiben und deshalb nicht behoben werden können. Sehr häufig werden bei einem Penetration Test Systeme entdeckt, von denen der IT-Leiter glaubt, dass sie längst nicht mehr betrieben werden. Wird ein veraltetes und nicht-gepatchtes System nicht abgeschaltet, haben Cyber-Kriminelle leichtes Spiel: Meist existiert bereits ein Exploit, über den sie das System übernehmen und für das weitere Ausbreiten im Netzwerk nutzen. Da solche Systeme auch mit dem internen Firmennetzwerk kommunizieren, können die Hacker von dort aus weitere Attacken starten – direkt in das Unternehmensnetzwerk hinein.

DIE AUFGABE

Für SER Group, Europas größten Software-Hersteller für Enterprise Content Management, hat Informationssicherheit größte Priorität. Mit der Durchführung eines Penetration Tests wollte das Unternehmen feststellen, wie gut es gegen Angriffe von außen geschützt ist – und beauftragte SVA mit einem „Extended“-Penetration Test über das Internet. Die Prüfer SVA sollten herausfinden, wie das Netzwerk von SER aufgebaut ist, die Netzwerkkomponenten analysieren, mögliche Schwachstellen identifizieren und Vorschläge zu ihrer Behebung liefern.

„Die Mitarbeiter der SVA haben mit uns direkt kommuniziert und uns über geplante Schritte im Vorfeld informiert, sodass wir im Störungsfall auch direkt den Pentest hätten stoppen können. Es war für uns eine angenehme und kompetente Zusammenarbeit.“

„Durch den Pentest wurden bei uns zum Glück keine größeren Sicherheitslücken festgestellt. Einige Dinge konnten wir jedoch im Nachgang ändern und wir haben die ein oder andere Sicht auf unsere Systeme dadurch verschärfen können. Wir werden die externen Pentests sicher weiter fortführen, um einer Betriebsblindheit vorzubeugen.“

DAS VORGEHEN

Aus Kundensicht ist ein externer Penetration Test durch SVA mit nur wenig Aufwand verbunden: Das Unternehmen muss lediglich die zu prüfenden IP-Adressen bzw. URLs benennen und die erforderlichen Zugangsdaten zur Verfügung stellen. Zum vereinbarten Termin machen sich die Prüfer ans Werk. Unmittelbar vor Beginn des Tests informieren sie noch einmal die IT-Verantwortlichen beim Auftraggeber, welche IP-Adresse getestet wird, um so die Wahrscheinlichkeit eines Impacts in den Produktivbetrieb zu reduzieren. Gibt es kritische Findings mit einem hohen Risiko, teilt SVA dies dem Kunden umgehend mit und liefert dabei eine ausführliche Beschreibung, wie die Schwachstelle aufgespürt wurde sowie Vorschläge, wie diese zeitnah beseitigt werden kann. Diese enge Kommunikation wusste auch SER sehr zu schätzen.

SVA setzt ausschließlich erfahrene und qualifizierte Mitarbeiter mit mehrjähriger Berufserfahrung im Bereich Pentesting ein, die als Offensive Security Certified Professional (OSCP) und Offensive Security Certified Expert (OSCE) zertifiziert sind. Statt wie oft üblich nur mit fertigen Tools automatisierte Scans durchzuführen, können die Prüfer von SVA manuelle Tests durchführen, die auch Zero-Day-Lücken aufdecken. Es handelt sich dabei um Schwachstellen, die noch in keiner Datenbank erfasst sind.
Der Penetration Test erfolgte in mehreren Stufen. Zunächst führte SVA einen automatisierten Scan der zur Verfügung gestellten IP-Adressen durch. Dabei zeigte sich, dass tatsächlich nur Systeme über das Internet erreichbar waren, für die dies vorgesehen ist – ein Beweis für die Wirksamkeit der mehrstufigen Security-Architektur, die SER betreibt.
SVA analysierte alle Dienste von SER, die aus dem Internet erreichbar sind, und stellte zum Beispiel fest, welches Betriebssystem verwendet wird, wie der Patch-Status ist und wann das letzte Update erfolgte. Die Spezialisten prüften anschließend manuell, ob es möglich ist, einen der vorhandenen Dienste wie Webservices, E-Mail oder Datenaustausch zu übernehmen – wie es ein Cyber-Krimineller tun würde.

DAS ERGEBNIS

Als Ergebnis erhielt SER ein detailliertes Risikoregister, in dem die Prüfer alle gefundenen Schwachstellen aufführten, beschrieben und bewerteten. Enthalten waren zudem konkrete Empfehlungen, wie sich die Schwachstellen beseitigen und so die Risiken erheblich reduzieren lassen. Darüber hinaus erhielt SER einen Abschlussbericht, der auch für sachverständige Dritte verständlich und nachvollziehbar ist. Die Ergebnisse des Penetration Tests wurden in einer Abschlusspräsentation vor Ort detailliert besprochen, die Vorschläge zur Behebung erörtert und gemeinsam Lösungen gefunden – die SER zeitnah umsetzte und damit die Sicherheitslücken schloss.

Der Penetration Test durch SVA verschaffte SER einen umfassenden Überblick über das aktuelle Sicherheitsniveau und leistete einen wertvollen Beitrag, um es weiter anzuheben – ohne dabei die Betriebsabläufe zu stören. SER zeigte sich sehr zufrieden mit der Zusammenarbeit mit SVA. Der durchgeführte Penetration Test hat entscheidend dazu beigetragen, die vorhandene IT-Infrastruktur noch sicherer zu machen und aufzuzeigen, an welchen Stellen sich in der Zukunft Handlungsbedarf ergeben könnte.

KONTAKT
SVA System Vertrieb
Alexander GmbH
Borsigstraße 14
65205 Wiesbaden
Tel: +49 6122 536-0
Fax:+49 6122 536-399
mail@sva.de
www.sva.de