LEIST OBERFLÄCHENTECHNIK PRÜFT SEIN SICHERHEITSNIVEAU MITTELS PENETRATION TESTS

AUF EINEN BLICK

Leistungsumfang

Ein Penetration Test ist die Simulation eines realen Cyberangriffs auf das Unternehmensnetzwerk. Hierfür bedienen sich die Penetration Tester von SVA derselben Tools und Methoden wie tatsächliche Hacker. Dadurch lässt sich ein detailliertes und realistisches Bild über das aktuelle Sicherheitsniveau des Unternehmens erzeugen. Des Weiteren dienen Penetration Tests der Überprüfung von Standards und Compliance-Richtlinien.

Nutzen

- Überprüfung des aktuellen Sicherheitsniveaus
- Aufdecken einer Zero-Day-Sicherheitslücke
- Definition von Maßnahmen zur weiteren Steigerung der IT-Sicherheit

IT-SICHERHEIT, EINE ZENTRALE HERAUSFORDERUNG

Die Anzahl der Cyberangriffe pro Unternehmen steigt kontinuierlich an. Gleichzeitig werden die Methoden der Angreifer technisch immer ausgefeilter. Hacker suchen nach Schwachstellen in öffentlich zugänglichen Netzwerken und Anwendungen, um in die Systeme eines Unternehmens einzudringen. Sobald der Zutritt gelungen ist, kann sich der Angreifer über weitere Schwachstellen im internen Netzwerk fortbewegen und möglicherweise an sensible Daten gelangen. Schwachstellen basieren überwiegend auf Fehlern in der zugrundeliegenden Software. Der Softwarehersteller stellt hierfür Patches bereit, die der zuständige Systemadministrator einpflegen muss. Andere Schwachstellen basieren auf Konfigurationsfehlern, welche nicht oder nur selten vom Hersteller gepatcht werden können. Hier bedarf es einer manuellen Anpassung.

Zum Auffinden derartiger Schwachstellen beauftragte die Leist Oberflächentechnik GmbH & Co. KG SVA mit einem Penetration Test. In diesem wurde das externe Netzwerk von Leist Oberflächentechnik untersucht. „Qualität, Sicherheit und Service – in Perfektion“ lautet das Leistungsversprechen des Spezialisten für die Veredelung von Oberflächen. Dem müssen auch die IT-Systeme entsprechend gerecht werden.

DEN NETZWERKSYSTEMEN AUF DEN ZAHN GEFÜHLT

Der Penetration Test war für Leist Oberflächentechnik mit wenig Aufwand verbunden. In einem vorbereitenden Gespräch wurden die Rahmenbedingungen geklärt. Anschließend wurden SVA die externen Netzwerkadressen mitgeteilt, die untersucht werden sollten. Die Penetration Tests von SVA sind so ausgelegt, dass diese den Betriebsablauf des Unternehmens nicht negativ beeinflussen und es somit zu keiner Ausfallzeit kommt. Destruktive Tests wie Brute-Force- oder Denial-of-Service-Angriffe (DoS) werden nur nach Absprache durchgeführt. Treten während eines Tests dennoch unerwartete Probleme auf, so sind die Kontaktpersonen seitens SVA jederzeit erreichbar.

leist
DAS ZENTRUM FÜR OBERFLÄCHENTECHNIK

Der Penetration Test bei Leist Oberflächentechnik wurde in verschiedene Phasen eingeteilt. Im ersten Schritt wurden alle aktiven Systeme, also solche, die über einen Dienst erreichbar sind, ermittelt. Dazu wurde ein Discovery Scan durchgeführt, bei dem alle 65.535 TCP-Ports geprüft wurden. Danach identifizierten die zertifizierten (OSCP/OSCE) Penetration Tester von SVA die eingesetzten Anwendungen, Betriebssysteme und Softwarestände und prüften diese manuell auf Schwachstellen. Im Gegensatz zu automatisierten Schwachstellen-Scans werden durch die manuelle Prüfung False-Positives, quasi ungerechtfertigte Fehlermeldungen, vermieden. Außerdem können durch den Einsatz spezieller Tools und manueller Recherche detailliertere Aussagen zu den Schwachstellen getroffen und passende Maßnahmen definiert werden.

AUF SICHERHEITSLÜCKEN KANN SOFORT REAGIERT WERDEN

Sobald die Prüfer von SVA während eines Penetration Tests eine kritische Schwachstelle erkannt haben, wurde Leist Oberflächentechnik direkt über diese informiert und erhielt darüber hinaus konkrete Vorschläge zur unmittelbaren Behebung der Schwachstellen. Die Tester wiesen jeder identifizierten Schwachstelle einen nachvollziehbaren Risikowert zu, indem sie diese mit Hilfe des Common Vulnerability Scoring v3.0 einordneten. Dadurch konnte Leist Oberflächentechnik unmittelbar auf die Bedrohungslage reagieren und die Ressourcen zur Behebung der Schwachstellen im Nachgang optimal steuern.

Nach Durchführung der Penetration Tests wurden Leist Oberflächentechnik ausführliche Beschreibungen sowie konkrete Empfehlungen zur Behebung der Schwachstelle gegeben. Diese Informationen wurden sowohl in Form eines Risikoregisters, als auch in einem ausführlichen Penetration-Test-Bericht zur Verfügung gestellt. In der Abschlusspräsentation haben die Penetration Tester von SVA den IT-Sicherheitsverantwortlichen von Leist Oberflächentechnik die Testergebnisse erläutert, und es wurden gemeinsam Lösungsansätze zur Steigerung des Sicherheitsniveaus diskutiert.

IM ERGEBNIS EINE WEITERE STEIGERUNG DES SICHERHEITSNIVEAUS

Durch den Penetration Test von SVA konnte eine Zero-Day-Sicherheitslücke in einem Videokonferenzsystem aufgedeckt werden. Der Hersteller dieses Systems wurde über diese Schwachstelle informiert und konnte sie mittlerweile schließen. Des Weiteren wurde das Sicherheitsniveau von Leist Oberflächentechnik schnell, realistisch und detailliert geprüft. Die konkreten Maßnahmen zur Schwachstellenbehebung konnte Leist Oberflächentechnik unmittelbar nutzen. Zusätzlich zum Penetration Test lieferte der Bericht Empfehlungen, welche Leist Oberflächentechnik als sehr nützlich für die weitere Steigerung des Sicherheitsniveaus empfand. Für die Folgeschritte und die Umsetzung der Punkte in einem technisch optimierten sowie wirtschaftlich gerechtfertigten Rahmen besteht ein enger Austausch zwischen den Verantwortlichen von Leist Oberflächentechnik und SVA.

Common Vulnerability Scoring v3.0
Kurz CVSS v3.0, verwendet einen Algorithmus, um unterschiedliche Werte für den Schweregrad einer Sicherheitslücke zu ermitteln. Die Einstufungen sind numerisch und reichen von 0,0 bis 10,0, wobei 10,0 die schwerste Sicherheitslücke darstellt.

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

DAS ZENTRUM FÜR OBERFLÄCHENTECHNIK