PENETRATION TEST LIEFERT KLARHEIT **KLEEMANN GMBH PRÜFT SEIN SICHERHEITSNIVEAU**

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.

Vorteile
- Überprüfung des aktuellen Sicherheitsniveaus
- Definition von Maßnahmen zur weiteren Steigerung der IT-Sicherheit

DIE AUFGABE

Tagtäglich sind Unternehmen Cyberangriffen ausgesetzt. Häufig suchen die Angreifer nach Schwachstellen in öffentlich zugänglichen Applikationen. Über Exploits lassen sich die gefundenen Schwachstellen automatisiert ausnutzen. So verschafft sich ein Angreifer mit geringem Aufwand Zugriff auf ein System des Unternehmens. Weitere Schwachstellen im internen Netzwerk ermöglichen es ihm, sich weiter im Netzwerk zu bewegen und an sensible Daten zu gelangen.

Schwachstellen basieren überwiegend auf Fehlern in der zugrundeliegenden Software. Der Hersteller der Software stellt Patches für diese bereit, die von dem zuständigen Systemadministrator eingepflegt werden müssen. Andere Schwachstellen basieren auf Konfigurationsfehlern. Diese können nicht oder nur selten vom Hersteller gepatcht werden und benötigen eine manuelle Anpassung.

Um solche Schwachstellen aufzufinden, beauftragte die Kleemann GmbH, ein mittständischer Baumaschinenhersteller mit Sitz in Göppingen, einen Penetration Test von SVA. In diesem sollten sowohl die externen, als auch die internen Netzwerke der Kleemann GmbH untersucht werden.

KLEEMANN

DAS VORGEHEN

Für die Kleemann GmbH war der Penetration Test mit wenig Aufwand verbunden. Nachdem Kunde und Dienstleister in einem Gespräch die Rahmenbedingungen geklärt hatten, teilten die Verantwortlichen den Testern von SVA die internen und externen Netzwerkadressen mit, die untersucht werden sollten. Die Penetration Tests von SVA sind so ausgelegt, dass sie den Betriebsablauf des Unternehmens nicht negativ beeinflussen und es somit zu keiner Ausfallzeit kommt. Destruktive Tests wie Brute-Force- oder Denial-of-Service-Angriffe werden nur nach Absprache durchgeführt. Treten während eines Tests dennoch unerwartete Probleme auf, so sind die Kontaktpersonen von SVA jederzeit erreichbar.

Der Penetration Test der Kleemann GmbH durchlief verschiedene Phasen. Im ersten Schritt ermittelten die Experten alle aktiven Systeme – das heißt solche, die über einen Dienst erreichbar sind. Dazu führten sie ein Discovery-Scan durch, bei dem sie alle 65.535 TCP-Ports prüften. Danach identifizierten die zertifizierten (OSCP/OSCE) Penetration Tester die eingesetzten Anwendungen, das Betriebssystem und die Softwarestände und prüften sie manuell auf Schwachstellen. Im Gegensatz zu automatisierten Schwachstellen-Scans schützt eine manuelle Prüfung vor False-Positives – auf gut Deutsch: vor falschem Alarm. Außerdem ermöglicht es der Einsatz spezieller Tools und manueller Recherche, detailliertere Aussagen zu den Schwachstellen zu treffen und passende Maßnahmen zu definieren.

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.

Die Tester ordneten jeder identifizierten Schwachstelle ein nachvollziehbares Risiko zu, indem sie diese mit Hilfe des Common Vulnerability Scoring v3.0 einordneten. Dadurch konnte die Kleemann GmbH die Ressourcen zur Behebung der Schwachstellen im Nachhinein optimal nutzen. Generell gilt: Erkennen die Prüfer von SVA während eines Penetration Tests kritische Schwachstellen, informieren sie den Kunden direkt. Zudem geben sie konkrete Vorschläge zur Behebung der Schwachstellen, sodass das Unternehmen unmittelbar auf die Bedrohungslage reagieren kann.

In einem weiteren Schritt lieferten die Experten von SVA Beschreibungen sowie konkrete Empfehlungen zur Behebung der Schwachstellen. Diese Informationen erhielt die Kleemann GmbH in Form eines Risiko-Registers als auch als ausführlichen Penetration-Test-Bericht. In der anschließenden Abschlusspräsentation besprachen Kunde und Dienstleister die Ergebnisse des Penetration Tests und diskutierten Lösungsansätze zur Steigerung des Sicherheitsniveaus.

DAS ERGEBNIS

Mit dem Penetration Test von SVA überprüfte die Kleemann GmbH ihr Sicherheitsniveau schnell, realistisch und detailliert. Die umfangreiche Auflistung aller aktiven Systeme verwendete sie später, um nicht mehr benötigte oder veraltete Systeme abzuschalten. Die konkreten Maßnahmen zur Beseitigung von Schwachstellen konnte sie direkt nutzen. Zudem lieferte der Bericht Empfehlungen zur weiteren Steigerung des IT-Security-Levels, was die Kleemann GmbH sehr begrüßte. Es besteht ein enger Kontakt zu SVA, um das Sicherheitsniveau im nächsten Schritt mit optimierten und wirtschaftlich vertretbaren Maßnahmen zu erhöhen.

KLEEMANN

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