Penetration Test

Der Test-Inhalt und die Vorgehensmethodik wurde einfach erklärt. Sehr umfangreiche Ergebnisse. Sinnvolle Massnahmen vorgeschlagen. Sehr gute Unterlagen
Xerox AG

Die Firma goSecurity GmbH hat mit ihrem kleinen, aber spezialisierten Team einen super Job gemacht. Sie arbeiten transparent und die Ergebnisse werden verständlich präsentiert.
EKU AG

Einleitung

Täglich werden neue Gefahren und Sicherheitslücken in Betriebssystemen und Applikationen entdeckt. Nur kurze Zeit später sind bereits Tools verfügbar, die diese Lücken ausnützen (Exploit). Alle Lücken zu kennen und entsprechend zeitgerecht zu schliessen, ist bei den täglichen Arbeiten und des grossen Zeitdrucks eines Administrators praktisch nicht mehr möglich. Zudem müssen viele Zugänge in der Firewall geöffnet sein (E-Mail, Web-Zugriffe, Partnerverbindungen, etc.). Daher ist es wichtig, das Maximum unternommen zu haben, um sich optimal vor diesen Gefahren zu schützen.

Inhalte

Externer Penetration Test
Der Penetration Test ist eine vollständige Kontrolle der von aussen erreichbaren Zugänge. Seien dies Verbindungen via Internet, Remote Zugänge (VPN) oder optional WLAN Access Points. Den Schwerpunkt bilden die Integrität, Vertraulichkeit und die Verfügbarkeit der erreichbaren Geräte. Folgende Bereiche werden untersucht:

:: Informationen über das Unternehmen
:: Verfügbare IP-Adressen
:: Offene Ports
:: Schwachstellen in der Firewall
:: Schwachstellen in der eingesetzten Software
:: weitere ausnutzbare Schwachstellen
:: Wireless Zugriffe (Kontrolle vor Ort, Optional)
:: Webseiten + Webapplikationen (Optional)

Interner Penetration Test
Beim internen Penetration Test stellen Sie uns wahlweise einen Arbeitsplatz zur Verfügung oder wir benutzen unsere Geräte. In der definierten Zeit versuchen wir den eingeschränkten Bereich zu verlassen und an vertrauliche Dokumente oder andere Informationen zu gelangen. Dies umfasst folgende Elemente:

:: Konfiguration des (mobilen) Arbeitsplatzes
:: Erreichbare Systeme
:: Schutz der (vertraulichen) Informationen
:: Citrix / Terminal Server Umgebungen

Nutzen

Erfahren Sie, wie weit unsere Experten in der Rolle eines Hackers in Ihre IT-Infrastruktur eindringen können. Mit diesem Wissen können Sie Schwachstellen gezielt schliessen. Ihre Kontrollfunktion nehmen Sie durch Penetration Tests optimal wahr und können dies (beispielsweise bei Revisionen) auch einfach belegen.

Vorgehen

Damit Sie optimal vom Penetration Test profitieren können, wird wie folgt vorgegangen:

:: **Informationen**
Sie geben uns nur diejenigen Informationen, die Sie herausgeben möchten. Die restlichen Informationen werden wir selber zusammentragen. In der Regel erhalten wir die zu überprüfenden IP-Adressen.

:: **Vorbereitungen**
Der erste Schritt umfasst die öffentlich zur Verfügung stehenden Informationen über Ihr Unternehmen. Mit einem Portscan untersuchen wir Ihre Umgebung. Welche Dienste reagieren bereits jetzt? Welche Informationen

geben uns diese Dienste zurück? Die gewonnenen Ergebnisse werden erfasst und mit Schwachstellen-Datenbanken verglichen.

:: **Dienste untersuchen**
Nach dem automatisierten Teil folgt die manuelle Kontrolle. Welche Dienste haben Schwachstellen? Wie können diese Schwachstellen ausgenutzt werden? Wie gelangen unsere Experten in Ihr Netzwerk? Welche Manipulationen können vorgenommen werden?

:: **Bericht**
Alle Informationen werden zusammengetragen und in einem Bericht ausführlich beschrieben. Nebst dem Vorgehen werden die gefundenen Schwachstellen aufgezeigt und in einer Massnahmenliste bewertet. Alle Resultate und weitergehenden Informationen finden Sie auf einem Datenträger.

:: **Präsentation / Besprechung**
Das Ergebnis des Penetration Tests wird Ihnen präsentiert und mit Ihnen besprochen. Sie wissen anschliessend, wo Sie die Hebel ansetzen müssen.

Resultate

Mit den Resultaten des Penetration Tests wissen Sie, welche Schwachstellen vorhanden sind und was Sie tun müssen, um sich optimal vor diesen Risiken zu schützen. Der Bericht enthält alle gefundenen Schwachstellen. Die Dokumentation ist so aufgebaut, dass Sie die Lücken selbstständig durch Ihre internen Fachkräfte oder Ihren vertrauten IT-Dienstleistungspartner schliessen können.

Zielgruppe des Penetration Tests

Der Penetration Test richtet sich an alle Firmen und öffentlichen Verwaltungen, die aus dem Internet erreichbaren Dienste selber betreiben (Web-, E-Mail-, FTP-Server, Remote-Zugänge, etc.). Dies ist unabhängig von der Branche oder der Grösse des Unternehmens. Der interne Penetration Test ist bestens geeignet für Firmen mit unterschiedlichen Mitarbeiterrollen (bezüglich Zugriffen) und Firmen mit vertraulichen Daten.

Kosten

Der Penetration Test dauert in der Regel zwischen 3 bis 8 Tagen. Dies ist abhängig von der Anzahl von aussen erreichbaren Diensten sowie den Informationen, die Sie uns zur Verfügung stellen. Sie erhalten den Penetration Test ab CHF 5'700.—.

Kontakt

Kontakt

goSecurity GmbH
Andreas Wisler
Schulstrasse 11
8542 Wiesendangen
052 320 91 20
info@goSecurity.ch
www.goSecurity.ch

Referenzen

AZ Direct AG
Hint AG, Lenzburg
BDO AG, Solothurn
EKU AG, Sirnach
Xerox AG, Kloten
Carbotech AG, Binningen
Atupri Krankenkasse, Bern
Rhenus Alpina AG, Basel
Burckhardt Compression AG, Winterthur
Jungfraubahnen Management AG, Interlaken
Technische Betriebe Wil
Paul Leimgruber & Co AG, Basel