



Einführung

Praktisch jeden Tag werden neue Gefahren und Sicherheitslücken in Applikationen und Betriebssystemen entdeckt. Nur wenige Augenblicke später sind bereits Tools verfügbar, die diese Lücken ausnützen. Alle Lücken zu kennen und entsprechend zeitgerecht zu schliessen, ist bei den täglichen Arbeiten eines Administrators praktisch nicht mehr möglich. Zudem müssen viele Zugänge geöffnet sein, da ansonsten beispielsweise kein Zugriff auf die Webseite möglich ist oder die Emails nicht empfangen werden können. 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 Zugängen, 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 verwendeten Software
- :: weitere ausnutzbare Schwachstellen
- :: Wireless Zugriffe (Kontrolle vor Ort, 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:

- :: Schutz des (eingeschränkten) Arbeitsplatzes
- :: Erreichbare Systeme
- :: Schutz der (vertraulichen) Informationen

Nutzen

Mit unserem Wissen und unserer Erfahrung versuchen wir kontrolliert in Ihre Infrastruktur einzudringen. Sollten wir Fehler oder Schwachstellen finden, werden diese detailliert erfasst und dokumentiert. Somit können Sie anschliessend die offenen „Türen“ schliessen oder die entsprechende Konfiguration vornehmen.

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 nur 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 können überwunden werden? Wie gelangen wir ins Netzwerk? Welche Manipulationen können wir vornehmen?

:: Bericht

Alle gefundenen Informationen werden zusammengetragen und in einem Bericht ausführlich beschrieben. Nebst dem Vorgehen werden die gefundenen Schwachstellen aufgezeigt und bewertet.

:: Präsentation / Besprechung

Das Ergebnis des Penetration Tests wird Ihnen präsentiert und vor Ort besprochen. Sie wissen anschliessend, wo Sie die Hebel ansetzen müssen.

Resultate

Mit den Resultaten des Penetration Tests wissen Sie, was Sie tun müssen, um sich optimal vor den Risiken zu schützen. Die Dokumentation enthält alle gefundenen Schwachstellen. Die Dokumentation ist so aufgebaut, dass Sie die Lücken selbstständig oder mit Ihrem IT-Betreuer schliessen können.

Zielgruppe des Penetration Tests

Der Penetration Test richtet sich an alle Firmen und öffentlichen Verwaltungen, die einen Internetanschluss haben und Dienste selber betreiben (Web-, Mail-, FTP-Server, Remote-Zugänge, etc.). Dies ist unabhängig von der Branche oder der Grösse.

Kosten

Der Penetration Test dauert in der Regel zwischen 3 bis 5 Tagen. Dies ist abhängig von der Anzahl von aussen erreichbaren Diensten sowie den Informationen, die Sie uns zur Verfügung stellen. Die Kosten bewegen sich in der Grössenordnung von Fr. 4800 - 8500.--.

Referenzen

Agtatec AG, Fehraltorf
Allgemeine Plakatgesellschaft, Winterthur
Allreal Generalunternehmung AG, Zürich
Axima AG, Winterthur
BDO Visura, Solothurn
Brauerei Schützengarten AG, St. Gallen
Embru Werke, Rüti
HINT AG, Aarau
Limmatdruck AG, Dietikon
MAAG Gear, Winterthur
Migros-Genossenschafts-Bund, Zürich
Pestalozzi+Co AG, Dietikon
Rahn AG, Zürich
Von Roll Umwelttechnik AG, Zürich

Kundenaussagen

Sehr gute Zusammenarbeit, Eingehen auf Kundenwünsche, Durchführung des Penetration Tests erfolgte wie abgemacht. Sehr gut gegliederter, nachvollziehbarer und verständlicher Bericht und Präsentation; man weiss anschliessend was zu tun ist. (Daniela Mohn, Limmatdruck AG)

Wir schätzten die professionelle, kompetente Zusammenarbeit mit der Firma GO OUT. Wir fühlten uns von Anfang an ernst genommen und haben genau das erhalten was wir erwartet haben. (Markus Sandhofer, Kaufmännisches Bildungszentrum Zug)

Kontakt

GO OUT Production GmbH
Schulstrasse 11
8542 Wiesendangen
Tel: 052 320 91 20
Fax: 052 320 91 21
info@goout.ch
www.goSecurity.ch

Ihre Ansprechpersonen

Andreas Wisler
Dipl. IT Ing. FH, CISSP, ISO 27001 Lead Auditor
MCITP Enterprise Server Administrator
wisler@goout.ch

Sandro Müller
Dipl. KI Ing. FH, Certified Ethical Hacker
mueller@goout.ch