

Ans Licht gebracht

von Sebastian Schreiber

Hochqualifizierte Experten attackieren ein Behörden-Netzwerk. Was sich für IT-Verantwortliche wie ein Albtraum anhört, ist als „Security Check“ eine echte Chance, vorhandene Sicherheitsschwächen zu identifizieren – und zu beseitigen.

Die Risiken, die in IT-Netzen lauern, werden von Unternehmen und Behörden meist vernachlässigt. Dabei beträgt das jährliche Wachstum der Computerkriminalität laut Statistik des Bundeskriminalamts etwa 300 Prozent. Die Dunkelziffer ist enorm, da Unternehmen aus Angst vor schlechter Publicity von einer Strafverfolgung Abstand nehmen. Doch die Frage, ob eine Straftat zur Anzeige gebracht werden soll, stellt sich einem Unternehmen oft gar nicht: Ein Opfer einer Hackerattacke weiß meist gar nichts vom Vorfall. Denn vertrauliche Daten sind schließlich noch da – auch wenn sie gestohlen wurden.

Für die Sicherheitsprobleme gibt es drei Ursachen:

1. Schlechte Softwarequalität. Hacker versuchen, Schwachstellen in Software zu finden. Dass sie dabei erfolgreich sind, ist kaum verwunderlich, da auch normale Anwender bei der täglichen Arbeit mit Software-Fehlern konfrontiert werden. Laut der Statistik des CERT Coordination Center werden pro Tag etwa zwölf neue Sicherheitslücken in Softwareprodukten bekannt – die Tendenz ist steigend. Keine Organisation ist in der Lage, auf solche Meldungen zeitnah zu reagieren. Für jede bekannt gewordene Sicherheitslücke ergibt sich also ein unvermeidbares Zeitfenster, in dem die Organisation verwundbar ist.

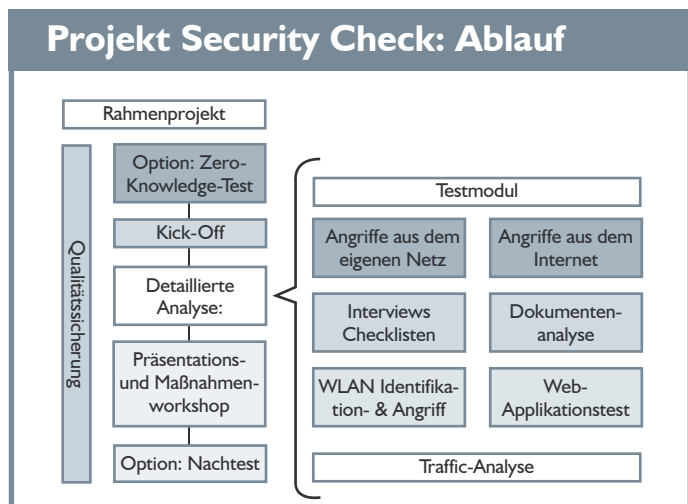
2. Know-how-Mangel. Da Fachkräfte Mangelware sind, greifen IT-Abteilungen meist auf Dienstleister zurück, deren

- Wie schaltet man unter Windows-2000 die Standardfreigaben dauerhaft ab?
- Wie funktioniert ein SYN-Cookie?
- Wie funktioniert die Zertifikatsüberprüfung für HTTPS unter Windows?
- Warum ist auf einem Windows-2000 Rechner der Port 445 offen und wozu wird er benutzt?

Werden alle Fragen korrekt und erschöpfend beantwortet, beherrscht der Administrator seinen Job. Leider kommt das nicht oft vor.

3. Zu niedrige Budgets. Gerade in wirtschaftlich angespannten Situationen werden bei IT-Security Einsparungspotenziale identifiziert. Welche Risiken Führungskräfte dabei eingehen, ist ihnen meist nicht bewusst.

Aufgrund der beschriebenen Rahmenbedingungen wird das „perfekte“ IT-Netzwerk wohl immer ein Traum bleiben. Das heißt aber nicht, dass man gar nichts tun kann, um sein Netz abzusichern. Der Security Check geht einen neuen, effizienten Weg: Ein kleines Team von hochqualifizierten Experten versucht, in einer definierten Zeit in einem Netzwerk befindliche Sicherheitsschwächen zu identifizieren. Der große Vorteil dieser Vor-





Hacker-Angriff: Häufig erfolgreich.

gehensweise ist die schnelle Verfügbarkeit und der geringe Zeitbedarf. Doch wie sieht ein Security Check aus? Um Sicherheitsschwächen zu identifizieren, gibt es eine Reihe unterschiedlicher Methoden:

Angriffe aus dem Internet: Sämtliche aus dem Internet erreichbaren Systeme werden auf Sicherheitsschwächen hin analysiert. Eine große Anzahl von Werkzeugen kommt zum Einsatz.

Angriffe aus dem eigenen Netzwerk: Unter Anwendung von mit Spezialwerkzeugen ausgestatteten Laptops wird versucht, vom Firmennetz aus Angriffe gegen kritische Systeme wie zum Beispiel Fileserver, Mailserver, PCs der Geschäftsführer, durchzuführen.

Dokumentenanalyse: Die Dokumentation der Infrastruktur wird sorgfältig analysiert.

Interviews: Mitarbeiter werden anhand von Checklisten befragt.

WLAN: Wireless LANs sind oft völlig ungesichert oder werden ohne Kenntnis der IT-Abteilung aufgebaut. Mit Spezialequipment werden solche WLANs identifiziert, analysiert und, falls erforderlich, lokalisiert.

Traffic-Analyse: Mit Spezialsoftware wird geprüft, welche Kommunikationsmechanismen eingesetzt werden. Insbesondere nach traditionellen, unverschlüsselten Protokollen wird gefahndet.

Welche der Module zum Einsatz kommen sollen, hängt stark von der Infrastruktur und den Sicherheitsanforderungen (=Schutzbedarf) der zu testenden Organisation ab. Das Projekt „Security Check“ gestaltet sich üblicherweise, wie in der Abbildung dargestellt. Darüber hinaus müssen weitere Parameter gesetzt werden, um den Erkenntnisgewinn zu optimieren:

Wissensstand: Hier kommen der Zero-Knowledge-Test (der Angreifer erhält keinerlei Wissen über das zu testende Netzwerk, er führt den Angriff also aus der authentischen Perspektive eines potenziellen Eindringlings durch) sowie der Whitebox-Test (der Angreifer enthält fundierte Informationen über das zu testende Netzwerk) zum Einsatz.

Aggressivität: Es wird versucht, unter Anwendung von Sabotage-

Attacken (so genannte D.o.S.-Attacken; D.o.S.= Denial of Service) Systeme zum Absturz zu bringen. Aber auch wenn auf Sabotage-Attacken verzichtet wird, kann die Funktion der zu testenden Systeme beeinträchtigt werden.

Testtiefe: Auf dem Plan stehen sowohl ein grober Test vieler Systeme, als auch ein fundierter, ausführlicher Test.

Ankündigung: Hier bestehen die Optionen „angekündigt“ und „unangekündigt“.

Der Security Check ist eine Dienstleistung, die sich in den letzten fünf Jahren in deutschen Unternehmen zu einem unverzichtbaren Standard entwickelt hat. Während Unternehmen in regelmäßigen Zyklen Security Checks durchführen lassen, nutzen Behörden diesen effizienten Weg zur Identifikation von Schwachstellen bislang kaum. Es ist davon auszugehen, dass sich dies in den nächsten Jahren ändern wird.

Sebastian Schreiber ist Geschäftsführer der SySS GmbH, Tübingen.

Pilot-Kommune gesucht

Kommune21 bietet in Zusammenarbeit mit dem Tübinger Beratungsunternehmen SySS ein Pilotprojekt für Kommunen an, mit dessen Hilfe durch gezielte Angriffe aus dem Internet oder auch innerhalb des kommunalen Netzwerks aktiv die IT-Sicherheit überprüft werden kann. Dafür wird eine Pilotkommune gesucht, die einen solchen Security Check bei sich durchführen lassen möchte. Über den Ablauf

und Ausgang dieses Projekts wird in einer späteren Ausgabe der Kommune21 berichtet – selbstverständlich anonymisiert. Die Pilotkommune erhält einen Rabatt von 50 Prozent auf die üblicherweise anfallenden Kosten. Nähere Informationen über die genaue Vorgehensweise und einen möglichen Projektablaufplan finden Sie unter

- www.kommune21.de/securitycheck