Ans Licht gebracht

Was man tun kann, um sein Netz abzusichern

Hochqualifizierte Experten attackieren die Netzwerke von Unternehmen oder Behörden. Was sich für IT-Verantwortliche wie ein Albtraum anhört, ist als Penetrationstest eine echte Chance, vorhandene Sicherheitsschwächen zu identifizieren und zu beseitigen.

Die Risiken, die in IT-Netzen lauern, werden von vielen Unternehmen und Behörden immer noch vernachlässigt. Laut Statistik des Bundeskriminalamts beträgt das jährliche Wachstum der Computerkriminalität etwa 300 Prozent. Die Dunkelziffer ist enorm, da Unternehmen aus Angst vor schlechter Publicity von einer – noch dazu wenig Erfolg versprechenden – 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 der Software zu finden. Dass sie dabei erfolgreich sind, ist kaum verwunderlich, da auch normale Anwender bei der normalen Arbeit täglich 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 Behörde und kein Unternehmen 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 Qualifikation oft nicht auf dem neuesten Stand ist. Die Anforderungen im Bereich IT-Security sind – auch aufgrund des ständigen Wandels der Netze und Betriebs-

systeme – sehr hoch. Allein folgende vier Fragen an Netzwerkadministratoren legen einige Wissenslücken offen:

- 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, dann beherrscht der Netzwerk-Administrator seinen Job. Leider kommt das nicht oft vor.

3. Zu niedrige Budgets

Gerade in wirtschaftlich angespannten Situationen werden bei der IT-Security Einsparungspotentiale 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 Penetrationstest 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 Vorgehensweise ist die schnelle Verfügbarkeit der Ergebnisse und der geringe Zeitbedarf. Doch wie sieht ein Penetrationstest 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 Notebooks wird versucht, vom Firmennetz aus Angriffe gegen kritische Systeme (zum Beispiel Fileserver, Mailserver, Personal Computer der Geschäftsführer) durchzuführen.
Dokumentenanalyse: Die Dokumentation der Infrastruktur wird sorgfältig analysiert.
Interviews: Mitarbeiter werden anhand von Checklisten befragt.
WLAN: WLANs sind oft völlig ungesichert oder werden ohne Kenntnis der IT-Abteilung aufgebaut. Mit Spezialequipment werden solche WLANs identifiziert, analysiert und lokalisiert.
Traffic-Analyse: Mit Spezialsoftware wird geprüft, welche Kommunikationsmechanismen eingesetzt werden. Insbesondere nach traditionellen, unverschlüsselten Protokollen wird gefahndet.

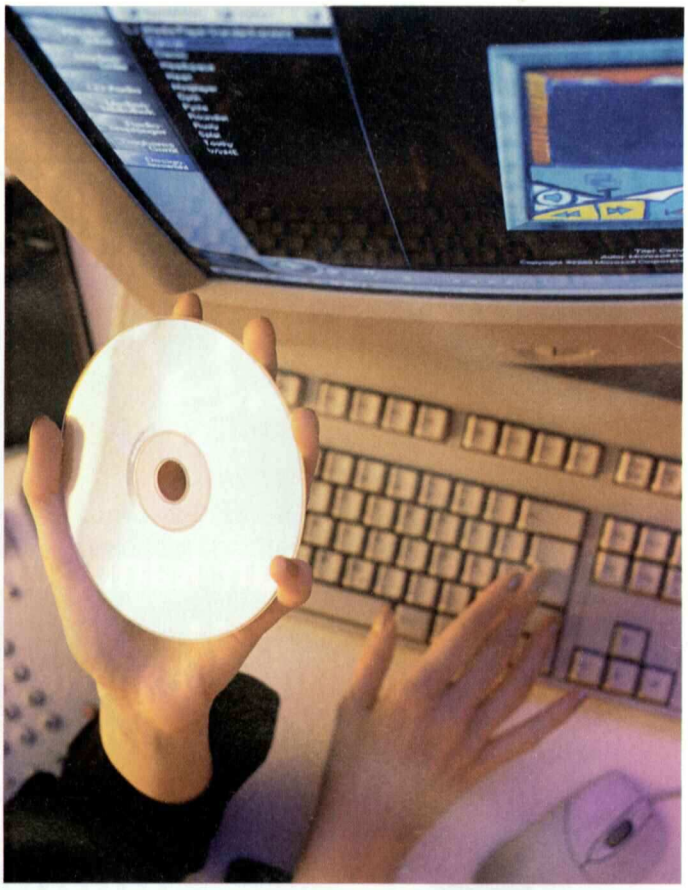

Foto: MEV

Welche der Module zum Einsatz kommen sollen, hängt stark von der Infrastruktur und den Sicherheitsanforderungen (=Schutzbedarf) des zu testenden Unternehmens ab. 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 erhält 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. 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: Der Penetrationstest kann angekündigt oder unangekündigt erfolgen.

Die während des Tests erlangten Kenntnisse werden dokumentiert. Tabellarisch werden sämtliche identifizierten Schwachstellen aufgelistet, mögliche Maßnahmen werden angesprochen. Der Penetrationstest ist eine Dienstleistung, die sich in den letzten Jahren zu einem wichtigen Standard entwickelt hat. Während Unternehmen in regelmäßigen Abständen Penetrationstests durchführen lassen, nutzen Behörden diesen effizienten Weg zur Identifikation von Schwachstellen bisher kaum.

Sebastian Schreiber