Lizenz zum Hacken.

IT-Systeme von Unternehmen und Organisationen sind immer wieder Ziel von Cyberattacken. Um dies zu verhindern, werden professionelle Hacker beauftragt, undichte Stellen aufzuspüren und Schutzschilder zu entwickeln. Eine Aufgabe für schlaue Köpfe mit tadellosem Leumund.

Nach der Jahrtausendwende wurden Sicherheitsprüfungen – oder Security Audits, wie sie in der Informatikbranche heissen – von zwei Arten Unternehmen angeboten: Entweder waren sie sehr technikorientiert, eher hemdsärmlige «Hackerfirmen», oder es waren Firmen, welche Security Audits nur als Türöffner anboten, um IT-Produkte zu verkaufen.

Reine Weste ist Pflicht

Heute wird der Schweizer Markt der Sicherheitstester im High-end-Segment von kleineren, auf derartige Dienstleistungen spezialisierten Firmen dominiert. Sie verfügen über Fachkompetenz und Erfahrung sowie über Teams mit tadellosem Leumund. Sie heissen beispielsweise Compass Security AG, ISPIN AG oder OneConsult GmbH.

Nichts vom gängigen Klischee

Das futuristische Äussere des Bürokomplexes der OneConsult GmbH und die konzentrierte Ruhe der Mitarbeiter an ihren Computern verströmen Seriosität und haben so gar nichts gemein mit dem Klischee des pickelgesichtigen Teenagers, der sich im abgedunkelten Raum die Nächte mit illegalen Hackversuchen um die Ohren schlägt.

Finger auf die wunde Stelle

60 bis 70 Prozent der Dienstleistungen sind IT-Sicherheitsaudits. Es sind Sicherheitsüberprüfungen mit dem Ziel, Schwachstellen aufzuspüren, das Sicherheitsniveau zu ermitteln und Gegenmassnahmen aufzuzeigen. Die restlichen 30 Prozent sind Beratung im IT-Security-Umfeld, Strategieberatung sowie Dienstleistungen wie Notfalleinsätze – wenn etwa eine Hackerattacke läuft oder eine Virenepidemie herrscht und ein Kunde externe Unterstützung benötigt. In diesem Zusammenhang bietet OneConsult auch adäquate Schulungen an.

IT-Fachchinesisch.

IT
Informationstechnologie

Security Scan
Automatisierte Sicherheitsprüfung mit manuellen Tests.

Penetration Test
Gründliche Sicherheitsprüfung mit hohem manuellem Test- und Verifikationsanteil.

Web Application Security Audit
Gründliche Sicherheitsprüfung eines Anwendungsprogramms und der zugehörigen Systeme.

Ethical Hacking
«Proof of Concept»-Auftragshacking, schützendes Hacken.

Patches
Nachbesserungen an Software oder SAP-Datenbanken.

Mainframes
Grossrechneranlagen z.B. für Banken, Volksabstimmungen etc.

Vier Augen sehen mehr

Die meistverlangte Dienstleistung ist der Penetration Test. Hier bewegt sich der manuell erbrachte Testanteil zwischen 60 und 70 Prozent. Der Löwenanteil der Prüfung geschieht manuell. Beim Thalwiler IT-Security-Spezialisten arbeiten daran meist zwei oder mehr Personen – aus der Erfahrung heraus, dass vier Augen mehr sehen als zwei. Es geht um Mailserver, Webserver oder Firewalls, aber auch um mobile Geräte wie Notebooks, Tablet-PCs und Smartphones.

Mittels Web Application Security Audits werden beispielsweise Internet-Banking-Lösungen und Onlineshops getestet. Dabei werden sowohl die firmenseitigen Systeme wie auch die beim Kunden verwendeten Komponenten (wie beispielsweise Apps oder Hardware für die Authentisierung) auf ihre Sicherheit überprüft.

Ethical Hacking

Der Ausdruck «Ethical Hacking» ist ein Versuch, sich vom Bad-Boy-Image des Hackers zu distanzieren. Beim Ethical Hacking handelt es sich um eine Art Nagelprobe, bei der aber oft nicht nach allen auf dem System befindlichen Sicherheitslücken gesucht wird. Im Fall von OneConsult wird dieser Test normalerweise nur in Kombination mit andern Testtypen angeboten, was zu einem besseren Mehrwert aus Auftraggebersicht führt.

Nur mit Erlaubnis

Aus rechtlichen Gründen ist es fast weltweit verboten, ein System ohne vorherige Genehmigung des Systemeigentümers zu testen. Beim konzeptionellen Security Audit geht es – im Gegensatz zum technischen Security Audit – darum, mittels Checklisten, Fragebögen, Interviews und/oder Dokumentationen die gelebten Sicherheitsprozesse, die Sicherheitsorganisation oder die Systemarchitektur zu prüfen. OneConsult zum Beispiel hat seit 2003 mehr als 400 technische Security Audits und Dutzende konzeptioneller Security Audits im In- und Ausland durchgeführt.

Vorschläge zur Verbesserung

Bei allen Security Audits erhält der Kunde neben der Auflistung gefundener Schwachstellen und dem angetroffenen Sicherheitsniveau auch eine Reihe von Empfehlungen, wie er die Lücken wirkungsvoll schliessen kann. Auf Betriebssystemebene betreffen die Massnahmen in den meisten Fällen Konfigurationsänderungen oder das unverzügliche Einspielen von Nachbesserungen, sogenannten Sicherheitspatches, welche nicht unmittelbar nach deren Veröffentlichung durch die Softwarehersteller eingespielt wurden. In manchen Fällen können aber diese Softwarekorrekturen nicht eingespielt werden, weil dies zu Inkompatibilitäten mit anderen Systemen führt. Bei Applikationen betreffen die meisten Mängel die fehlende Identitätsprüfung der Benutzer, die inkorrekte Benutzerrechteverwaltung oder die fehlerhafte Validierung von Benutzereingaben.