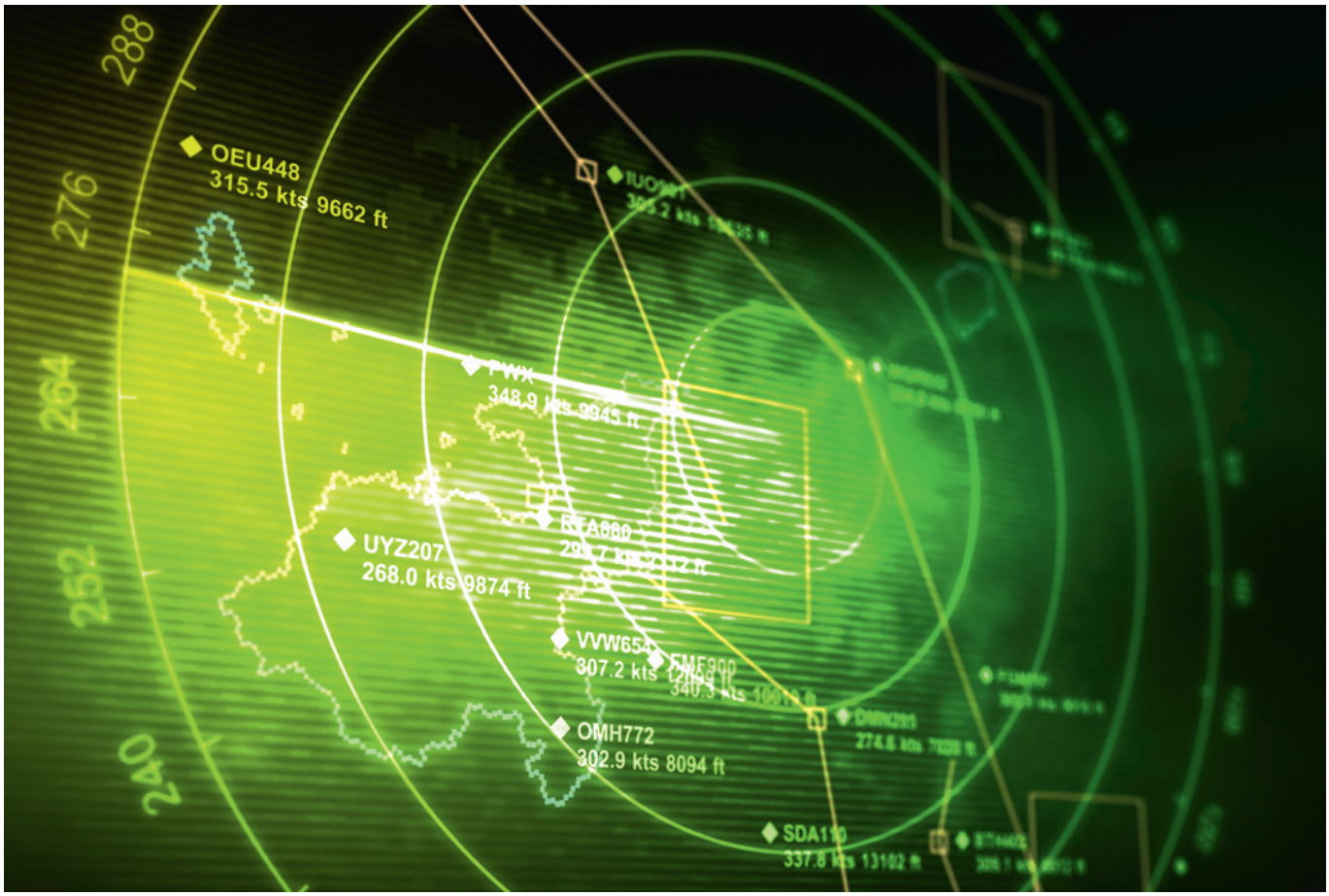
AUF DEM RADAR

SICHERHEITSSTRATEGIEN IN DER PRAXIS

von Andreas Wisler

Erfahrungen aus IT-Security Audits gehen in ziemlich eindeutige Richtungen und lassen sich relativ schnell und einfach in praktische Massnahmen umsetzen.



Die vergangenen Monate haben gezeigt, das Interesse an Daten und Informationen ist ungebrochen hoch. Fast täglich ist von Passwort- und Datendiebstählen zu lesen. Aber nicht nur Hacker und Cracker möchten mit diesen Daten Geld verdienen, auch staatliche Organisationen haben grosses Interesse an Informationen. Daher ist es weiterhin wichtig, seine Daten zu schützen und nicht den Kopf mit der Begründung «Ich kann ja doch nichts machen» hängen zu lassen.

ORGANISATORISCHE MÄNGEL

Die IT ist Unterstützer der Business-Prozesse. Auch wenn die IT-Verantwortlichen dies nicht gerne hören, ist die IT-Umgebung «nur» dazu da, das Business optimal zu unterstützen und damit erst zu ermöglichen. Aber um diese Aufgabe erfolgreich umzusetzen, muss die IT die Prozesse kennen. Das bedeutet, dass die Geschäftsleitung diese transparent (und in einer für die IT geeigneten Sprache) aufzeigen muss. Wir empfehlen hier unbedingt eine IT-Strategie, gestützt auf die vorhandenen Prozesse, zu erstellen. Aus diesem Dokument muss herauskommen, wie kritisch einzelne Prozessschritte sind, welche Verfügbarkeit gefordert, welche Ausfalldauer akzeptiert und welcher maximale Datenverlust verkraftet werden kann. Daraus leitet sich für die IT die technische Umsetzung ab. Unsere Audit-Erfahrungen zeigen, dass hier zu wenig miteinander gesprochen wird und daher einige IT-Projekte nicht zur Zufriedenheit der Geschäftsleitung umgesetzt werden.

SOCIAL ENGINEERING

Obwohl in den vergangenen Wochen sehr viel über diese Angriffsart gelesen werden konnte, ist es doch erstaunlich, wie einfach man über diesen Weg an Informationen gelangt. Ein klassisches Beispiel ist der Aufruf an alle Mitarbeiter, an einer Umfrage zum Umgang mit Passwörtern mitzumachen. Wenn das E-Mail noch den Absender des obersten Chefs trägt und ein dicker Preis winkt, ist die Hürde klein, hier mitzumachen. Doch gerade dann ist grosse Vor-

sicht geboten. Geht der Link wirklich auf das Intranet, oder wurde die Umfrage-Webseite nur gut nachgemacht? Unsere Angriffe, in Absprache mit den verantwortlichen Personen, zeigen eine sehr hohe Erfolgsquote, meistens über 60 Prozent der Angeschriebenen können der Versuchung nicht widerstehen und klicken auf den Link.

Doch auch weitere Quellen können der Informationssuche dienen. Viele Menschen sind sehr unvorsichtig im Umgang mit den eigenen Daten. So können via Xing, Linkedin, Facebook oder der eigenen Webseite bereits sehr viele Informationen zusammengetragen werden. Verschiedene spezialisierte Suchmaschinen nehmen dem potenziellen Angreifer die Arbeit ab und durchsuchen verschiedene Quellen auf einmal und stellen die Informationen übersichtlich dar.

EXTERNE SICHT

Beim Penetration-Test geht es darum, einen Weg in die Firma zu finden. Auch hier helfen sogenannte Erfolgsgeschichten von Herstellern, Beschreibungen auf der Firmenwebseite und vor allem Stelleninserate, welche aufzählen, was für technische Fähigkeiten der neue Mitarbeiter haben muss. Mittels IP- und Portscans können weitere Informationen dazukommen. Vor allem Bannerinformationen von erreichbaren Servern sollten, falls immer möglich, verhindert werden. Gibt der Dienst die genaue Version an, kann in Schwachstellendatenbanken nachgesehen werden, ob bereits eine bekannte Angriffsfläche vorhanden ist, die für einen weiteren Schritt (aus-)genutzt werden kann. Auch gilt es, Firewall-, Router- oder gar Remotezugänge nicht von aussen erreichbar zu konfigurieren. Werden fehlerhafte Login-Versuche nicht ausgewertet oder erkannt, kann der Angreifer in Ruhe versuchen, an das richtige Passwort zu gelangen.

INTERNE SICHT

Kennen Sie die Bilder von Kabeln, die kreuz und quer durch den Serverraum führen? Immer wieder sehen wir dies in unseren Audits. Das macht die Fehlersuche bei Problemen enorm aufwendig. Auch wird der Serverraum gerne als Lagerraum zweckentfremdet. Dies erhöht die Brandlast und sollte daher tunlichst vermieden werden.

Schwachstellen kommen in jeder Software vor. Früher oder später werden diese entdeckt. Daher ist es enorm wichtig, dass das Patchmanagement sauber und regelmässig durchgeführt wird. Jedoch gilt dies nicht nur für das Betriebssystem, auch die installierten Applikationen benötigen ein Update. Dies ist eine der wichtigsten Aufgaben des Administrators und darf unter keinen Umständen vernachlässigt werden!

Die Übertragung von Daten wie Passwörter wird zum Glück vermehrt über verschlüsselte Verbindungen sichergestellt (erkennbar am HTTPS). Aus Kostengründen werden aber auch selber erstellte Zertifikate benutzt. Das Problem an diesen Zertifikaten ist die erscheinende Fehlermeldung. Alle aktuellen Browser weisen prägnant auf diesen Missstand hin. Werden die Benutzer geschult, diese Fehlermeldung zu ignorieren, wird ein falsches Bild vermittelt. Erscheint diese Fehlermeldung nun beim Aufruf des Online-Banking, wird gewohnheitsmässig auf «Weiter» geklickt, anstelle die Verbindung sofort abzubrechen. Daher empfehlen wir immer, offizielle Zertifikate anzuwenden, bei welchen keine Fehlermeldung auftritt.

Ein weiteres Problem ist die zu grosszügige Vergabe von Zugriffsrechten. Werden unter Windows gar die Rechte «Vollzugriff» vergeben, kann der Benutzer selber weiteren Personen Zugriff gewähren. Ein sauberes Freigabe- und Berechtigungskonzept kann dies verhindern. Bei Stichproben finden wir gelegentlich auch sensible Daten in diesen Verzeichnissen wie Softwareschlüssel, Backupdaten, persönliche Informationen oder Buchhaltungsdaten. Diese Daten sollten aber unter keinen Umständen in die falschen Hände gelangen.

Cloud-Dienste sind smart und einfach zu nutzen. Doch geschäftliche Informationen gehören hier nicht hin. Hat der Benutzer auf seinem Gerät die notwendigen Rechte, weitere Software zu installieren, wird gerne zu Dropbox oder anderen Cloud-Speichern gegriffen. Und schon werden interne Daten zur einfachen Bearbeitung über diese Medien ausgetauscht.

FAZIT

Der Administrator hat eine wichtige Aufgabe. Er muss sich um die Angriffsfläche von aussen kümmern und alle Lücken schnellstmöglich schliessen. Aber auch von intern «droht» die Gefahr. Nicht Absicht steht hier an erster Stelle, sondern Unwissenheit, Fahrlässigkeit oder einfach «Faulheit». Daher gilt es, das Angriffspotenzial so klein wie möglich zu halten. Dazu gehört neben einer IT-Strategie und einem IT-Sicherheitskonzept auch ein regelmässiges Patchmanagement. Die Benutzer müssen auf die vorhandenen Gefahren sensibilisiert und Möglichkeiten zum sicheren Umgang mit IT-Mitteln aufgezeigt werden. Auch mit den aktuell vorhandenen Gefahren ist es möglich, die eigene IT-Umgebung sicher zu betreiben. ■

Welche Wege gibt es in das Unternehmen für ungebetene Besucher?

ANDREAS WISLER

ist CEO und Senior Security Consultant von goSecurity.

www.gosecurity.ch