Lassen Sie sich hacken: IT-Sicherheitslücken offensiv angehen

Digitalisierung & IT

IT-Sicherheitsvorfälle respektive Cybercrime sind inzwischen in deutschen Unternehmen nahezu alltäglich. Gerade der Mittelstand ist mittlerweile stark von Datenklau bzw. Datendiebstahl betroffen. Trotz dieser stetigen Konfrontation mit dieser Thematik herrscht offenbar immer noch eine gewisse Arglosigkeit in den Führungsetagen der mittelständischen Unternehmen vor; das Gefahrenpotenzial einer expliziten Internet-Kriminalität wird in vielen Betrieben unterschätzt. Das ist ein schwerwiegender Fehler, denn zwischen einem funktionellen Daten- und Informationssicherheit-Management und dem wirtschaftlichen Erfolg bzw. dem Wertschöpfungsprozess an sich besteht eine nachhaltige Verbindung.

Michael Wolf

Kooperationspartner
Johannes Müller
Wirtschaftsberatung (BDU)

IT-Spezialist
IT-Architekt
Penetrationstests

Unternehmen oft Selbstbedienungsladen für Datendiebe

Dass gerade die kleinen und mittelständischen Unternehmen in den Fokus der Cyber-Kriminellen gerückt sind, ist verständlich. Schließlich gelten gerade diese Unternehmen in Deutschland als explizite Know-how-Träger. Ob Konstruktionszeichnungen, Patent- und Prozessbeschreibungen, Kalkulationen, Kundenlisten, Ausschreibungen und Angebote sowie natürlich der E-Mail Verkehr mit Geschäftspartnern, Lieferanten sowie Kunden - keine Frage, dort gibt es auch eine Menge zu holen. Sicherheitsexperten heben hier schon länger den warnenden Zeigefinger und sehen die IT-Infrastruktur in etlichen Unternehmen aufgrund von fehlenden bzw. nicht ausreichenden Sicherheitsmaßnahmen als „Selbstbedienungsladen" verkommen.

Immer noch werden einzelne Bereiche vernachlässigt

Sicherheitsmaßnahmen sind längst nicht überall in genügendem Maße etabliert. Sind Firewalls einmal eingerichtet worden, arbeiten sie oft jahrelang, ohne eine regelmäßige Wartung und Pflege. Optimaler Schutz sieht anders aus.

„Um Sicherheitslücken aufzuzeigen, sollten sich Unternehmen auf Bestellung hacken lassen. Die Erkenntnisse daraus sind Gold wert, weil Defizite gezielt behoben werden können."

Michael Wolf, Kooperationspartner Johannes Müller Wirtschaftsberatung (BDU)

Nicht nur Firewall und Co. werden vernachlässigt behandelt. Auch zahlreiche Serversysteme, die quasi das Rückgrat einer jeden Firmen-IT bilden, arbeiten teilweise über mehrere Jahre hinweg, ohne dass Updates aufgespielt werden oder auch ohne dass eine kontinuierliche Kontrolle der Log-Dateien erfolgt.

Zentral organisierte Kontrollen von Endgeräten fehlen nahezu gänzlich

Zwar werden Szenarien dieser Art immer seltener, da die Server mittlerweile eingehender auf Schwachstellen untersucht werden. Dafür werden dann aber wiederum die Kontrollen der Endgeräte vernachlässigt. Hier wird eindeutig zu wenig Fokus auf eine umfassende Endpoint-Security gelegt. Im Optimalfall sollte eine zentral organisierte Kontrolle generiert werden. Auch wenn Geräte Dienste bereitstellen, die außerhalb des eigenen IT-Firmennetzwerks liegen, wie zum Beispiel SSH, FTP, VPN, Web-Server oder etwa die in Firmen stark genutzten Dokument-Managementsysteme, mangelt es an entsprechend spezifischen Sicherheitsvorkehrungen bzw. -maßnahmen.

Hohes Gefahrenpotenzial: Keine veraltete Software nutzen

Hinzu kommt, dass auf vielen Servern Anwendungen und Dienste laufen, die eigentlich gar nicht benötigt werden. Da sie überhaupt nicht beachtet werden, sind sie häufig mangelhaft bzw. fehlerhaft konfiguriert und weisen entscheidende Sicherheitslücken auf. Potentielle Angriffspunkte können zudem durch veraltete Software entstehen.

„Das Betriebssystem Windows XP hat nichts mehr auf den Geräten eines Unternehmens verloren. Der Support endete bereits 2014. Wer jetzt noch damit arbeitet, geht ein hohes Sicherheitsrisiko ein."

Michael Wolf, Kooperationspartner Johannes Müller Wirtschaftsberatung (BDU)

Gleiches gilt etwa auch für Server Betriebssysteme, die nicht mehr den modernen Ansprüchen genügen. Entsprechend veraltete Software sollte daher ebenfalls grundsätzlich ausgetauscht werden, sofern keine neuen Sicherheitsupdates mehr zur Verfügung stehen.

Vorsorge und Prävention als entscheidende Faktoren

IT-Sicherheitsvorfälle bzw. gezielter Datenklau können meistens bereits im Vorfeld verhindert werden. Prävention und Vorsorge sind entscheidende Faktoren zur Vermeidung von Cyber-Kriminalität. Dazu gehört auch die Möglichkeit, die eigenen Sicherheitslücken durch selbst initiierte Hackerangriffe zu prüfen. Der Umgang damit und die daraus resultierenden Maßnahmen für ein effektives Sicherheitsmanagement-System sind entscheidende Faktoren. Passiert dann doch einmal was, sollten schnelle und dabei auch vergleichsweise kostengünstige Wege der Wiederherstellung zur Verfügung stehen.

Trotzdem sollte sich ein Unternehmen nicht zu sicher fühlen. Denn nicht bei allen Hacker-Angriffen handelt es sich um leicht zu identifizierenden Virusbefall oder etwa um Verschlüsselungstrojaner. Oftmals sind Firmen-Computer mit Schadsoftware verseucht, die unauffällig im Hintergrund Daten ausspioniert. Aber auch hier kann das Risiko zumindest reduziert werden. Dafür müssten die IT-Verantwortlichen lediglich die jeweiligen Protokolldateien regelmäßig und systematisch auswerten lassen.