Top 10 Bedrohungen der Datensicherheit bei KMUs

Der folgende Artikel ist ein Auszug aus dem White Paper mit dem Titel *Top Ten Security Threats for SMEs (and what to do about them)* von Scott Pinzon, CISSP, vom WatchGuard®-LiveSecurity®-Team. Wir stellen darin die häufigsten zehn Bedrohungen für die Netzwerksicherheit und eine mögliche Abwehrmaßnahme vor. Genauere Infos zu Auswahlkriterien, Netzwerktyp sowie mindestens zwei Gegenmaßnahmen pro Bedrohung finden Sie im kompletten White Paper unter www.watchguard.com/whitepapers, das Sie kostenlos herunterladen können.

Die Erfassung verlässlicher und vor allem aktueller Daten zur Definition von Netzwerkbedrohungen gestaltet sich als äußerst schwierig.

So untersucht das WatchGuard-LiveSecurity-Team seit 1999 täglich neue Bedrohungen, die speziell für kleine und mittlere Unternehmen (KMUs) zum Problem werden können. Da wir wissen, dass unsere Abonnenten oft unter Zeitdruck und hoher Belastung stehen, geben wir nur dann eine Warnmeldung aus, wenn eine Bedrohung nicht nur möglich, sondern wahrscheinlich ist. Diese Fokussierung auf geschäftliche Aspekte und Praktikabilität ist es, was unseren Service so einzigartig macht. Dazu kommt, dass wir unsere Wissensbasis ständig mit dem Feedback Zehntausender Abonnenten, Kundenbesuchen sowie über Fokusgruppen und informelle Diskussionsrunden erweitern.

Das Ergebnis ist eine Liste mit 10 Bedrohungen, die nach unseren Erfahrungen als Analysten in diesem Bereich das größte Risiko für die Datensicherheit bei KMUs darstellen. Ergänzt wird diese Aufstellung durch praktische Techniken und Abwehrmaßnahmen.

Bedrohung Nr. 10: Insiderattacken

Das Intrusion-Response-Team von Verizon hat in 4 Jahren 500 Attacken untersucht und davon 18 % auf Sicherheitsverletzungen durch Insiderattacken zurückgeführt, von denen die Hälfte wiederum auf EDV-Mitarbeiter entfällt.[1]

Maßnahme gegen Insiderattacken

Implementierung des Prinzips der doppelten Kontrolle. Voraussetzung hierfür ist, für jede wichtige Ressource eine Absicherung bereitzustellen. Wenn z. B. ein Mitarbeiter primär für die Konfiguration von Web- und SMTP-Servern zuständig ist, sollten die Anmeldedaten für diese Server mindestens einer weiteren Person bekannt/zugänglich sein.

Bedrohung Nr. 9: Fehlende Strategien für den Ernstfall

Unternehmen, die als Geschäftsvorteile Schnelligkeit und Ansprechbarkeit auflisten, erreichen diese nicht selten durch den Verzicht auf standardisierte und durchdachte Prozesse sowie Notfallstrategien. Viele KMUs haben so schon erfahren müssen, dass einfache Datenfehler oder Sicherheitsverletzungen ohne Business-Continuity-/Disaster-Recovery-Plan, Intrusion-Response-Richtlinie, aktuelle und *tatsächlich funktionierende* Backupsysteme oder Offsite-Speicherlösungen katastrophale Folgen haben können.

Maßnahme gegen fehlende Strategien für den Ernstfall

Wenn Sie über ein entsprechendes Budget verfügen, sichern Sie sich unbedingt die Dienste eines Experten zur Entwicklung ausgereifter Informationssicherungsmethodologien. Im anderen Fall nutzen Sie das Wissen Dritter als Grundlage für firmeneigene Prozesse, wie z. B. das SANS Security Policy Project mit seinen kostenlosen Vorlagen

[1] Zusammenfassung unter http://www.infosectoday.com/Articles/2008_Data_Breach_Investigations_Report.htm. Eine PDF-Datei dieses Berichts finden Sie unter http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

und Ressourcen zur Erstellung eigener Richtlinien. Weitere Infos finden Sie unter http://www.sans.org/resources/policies/.

Bedrohung Nr. 8: Unzureichende Konfiguration als Sicherheitsrisiko

KMUs mit wenig Erfahrung und begrenzten Finanzressourcen setzen nicht selten Router, Switches und andere Netzwerkgeräte ein, verfügen aber über keine Mitarbeiter, die sich mit den sicherheitstechnischen Aspekten dieser Hardware auskennen. So kann es sein, dass sich ein unerfahrener Netzwerktechniker mit der Bereitstellung einer einwandfreien Datenübertragung begnügt und dabei vielleicht versäumt, die standardmäßigen Benutzernamen und Anmeldedaten des Herstellers zu ändern.

Maßnahme gegen eine unzureichende Konfiguration

Durchführung eines automatisierten Vulnerability-Audit-Scans. Auch wenn Sie sich keine Fachkräfte leisten können, gibt es immer noch Vulnerability-Management-Programme, mit denen Sie im Rahmen Ihrer routinemäßigen Netzwerkwartung automatisierte Scans Ihres Netzwerks durchführen können. Diese Produkte werden in großer Vielfalt und in allen Preisklassen angeboten.

Bedrohung Nr. 7: Unbedachte Nutzung von Hotel-Netzwerken und Kiosks

Hotelnetzwerke bieten selten ausreichenden Schutz oder geeignete Sicherheitspraktiken gegen Viren, Würmer, Spyware und Malware. Öffentliche Kiosks laden Angreifer geradezu dazu ein, Keylogger zu installieren und wie eine Spinne im Netz auf ahnungslose Opfer zu warten. So sind Laptops ohne aktuelle Firewall, Antivirus-Programme oder Anti-Spyware besonders im mobilen Einsatz hochgefährdet. Traditionelle Abwehrmaßnahmen bleiben wirkungslos, wenn der Benutzer sein Gerät außerhalb der Gateway-Firewall verwendet hat und dann eine Verbindung innerhalb der Trusted Zone herstellt.

Maßnahme gegen die unbedachte Nutzung von Hotel-Netzwerken

Einrichten / Durchsetzen von Richtlinien gegen die Deaktivierung von Schutzmaßnahmen durch Mitarbeiter. Laut einer von Fiberlink in Auftrag gegebenen Studie hat einer von vier mobilen Mitarbeitern zugegeben, die Sicherheitseinstellungen auf seinem Laptop geändert oder deaktiviert zu haben. Sie sollten deshalb eine Richtlinie implementieren, die Ihren Mitarbeitern solche Aktionen ohne entsprechende Genehmigung untersagt. Viele gängige Antiviruslösungen lassen sich außerdem so konfigurieren, dass sie selbst von Benutzern mit Administratorprivilegien nicht deaktiviert werden können. Prüfen Sie, ob Ihre Lösung über eine solche Funktion verfügt.

Bedrohung Nr. 6: Unbedachte Nutzung von WiFi-Hotspots

Öffentliche Wireless-Hotspots sind noch gefährlicher als Hotelnetzwerke. So müssen Angreifer lediglich einen solchen Hotspot als "kostenloses öffentliches WiFi" einrichten und auf unvorsichtige Nutzer warten, deren Eingaben (z. B. Anmeldungen) sie dann mit Hilfe eines aktivierten Packet Sniffers mühelos ausspionieren können. Es handelt sich hier um eine besonders hinterhältige Attacke, da aufgrund der Drahtlos-Verbindung *keinerlei Spuren* einer Sicherheitsverletzung auf dem PC des Opfers verbleiben.

Maßnahme gegen eine unverantwortliche WiFi-Nutzung

Weisen Sie Ihre Benutzer auf die Wichtigkeit verschlüsselter Verbindungen hin. Machen Sie die Verwendung von Virtual Private Networks (VPNs) zur Pflicht, bei denen der Datenstrom verschlüsselt wird und so von Dritten nicht verwertet werden kann.

Bedrohung Nr. 5: Datenverlust auf tragbaren Geräten

Jedes Jahr gehen Unmengen an wertvollen Informationen verloren, weil Anwender z. B. ihr Smart Phone im Taxi, den USB-Stick im Hotel oder den Laptop im Zug vergessen. Zum Schutz von Daten auf Kleingeräten sollten sich Administratoren deshalb nicht mit der Frage befassen, *ob* ein Gerät verloren geht, sondern *was im Ernstfall zu tun ist*.

Maßnahme gegen Datenverlust auf tragbaren Geräten

Zentrale Verwaltung von Mobilgeräten. Investieren Sie in Server und Software, mit denen Sie Mobilgeräte zentral verwalten können. Mit dem Blackberry Enterprise Server von RIM z. B. können Sie Datenübertragungen verschlüsseln und bei Verlust eines Geräts sogar Inhalte per Remote-Verbindung löschen. Mit solchen Maßnahmen können Sie alle möglichen Risiken für den Ernstfall erheblich mindern.

Bedrohung Nr. 4: Angriffe auf Webserver

Die häufigsten Botnetz-Attacken richten sich gegen Websites. Sie sind deshalb oft erfolgreich, weil die meisten Sites mit anfälligem Applikationscode geschrieben wurden. So konnten Bot Master mit automatisierten SQL-Attacken bereits Hunderttausende von Servern auf einen Schlag infizieren und legitime Sites zur Verbreitung von Malware missbrauchen.

Maßnahme gegen Angriffe auf Webserver

Prüfen Sie Ihren Applikationscode. Wenn z. B. ein Webformular ein Feld für die Eingabe einer Telefonnummer enthält, sollte die Webapplikation eine Funktion zur automatischen Löschung überzähliger Zeichen enthalten. Wenn die Applikation für bestimmte Daten oder Befehle keine Routinen enthält, muss deren Bearbeitung abgelehnt werden. Scheuen Sie bei der Auswahl der geeigneten Code-Auditing-Lösung (egal ob Expertenteam oder automatisiertes Tool) keine Kosten und prüfen Sie, ob sich eine korrekte Eingabeverifizierung durchführen lässt.

Bedrohung Nr. 3: Unbedachtes Websurfing durch Mitarbeiter

Laut einer 2006 durchgeführten Studie der Universität Washington sind die Top 3 Websites, die am meisten Spyware verbreiten:

1. Star-Fan-Sites (z. B. mit aktuellen und doch sinnlosen News über Paris Hilton und Britney Spears)
2. Casual-Gaming-Sites (wo man z. B. gegen andere Benutzer Schach oder Snooker spielen kann)
3. Porno-Sites (überraschenderweise nur auf Platz 3)

Auf Social-Networking-Sites wie MySpace und Facebook tun sich mittlerweile tiefe Sicherheitsabgründe in Sachen Bedrohungen auf. So kann es sein, dass man beim privaten Surfen während der Arbeit Bot-Clients, Trojanern, Spyware, Keyloggern, Spambots, also praktisch der ganzen Bedrohungspalette Tür und Tor zum Firmennetzwerk öffnet.

Maßnahme gegen unbedachtes Websurfing

Implementieren von Webcontent-Filtern. Nutzen Sie Webfiltering-Software wie den WatchGuard WebBlocker, die täglich aktualisierte Datenbanken mit blockierten URLs in zahlreichen Kategorien verwenden. Je mehr Kategorien, desto höher die Sicherheit. Mit solchen Werkzeugen lassen sich sehr einfach Richtlinien, die auch von Benutzern akzeptiert werden, durchsetzen.

Bedrohung Nr. 2: Bösartige HTML-Mails

Die häufigsten Attacken werden in Form von HTML-Mails ausgeführt, deren Links auf tückische Webfallen verweisen. Schon ein einziger falscher Klick kann so einen Drive-by-Download auslösen. Diese Bedrohung ähnelt der für unbedachtes Websurfing, mit dem Unterschied, dass das Opfer hier per E-Mail zur bösartigen Website gelotst wird.

Maßnahme gegen bösartige HTML-Mails

Implementieren eines Outbound-Webproxys. Sie können Ihr LAN so einstellen, dass alle HTTP-Anforderungen und -Antworten an einen Webproxy-Server geleitet werden, der den Datenverkehr zentral überwacht. Zwar wirkt diese Maßnahme nicht gegen eingehende bösartige E-Mails, allerdings verhindert sie effektiv, dass abgehende HTML-Anforderungen überhaupt bei bösartigen Websites ankommen.

Bedrohung Nr. 1: Automatisierter Angriff auf eine bekannte Schwachstelle

Der *Data Breach Investigations Report 2008* von Verizon listet Fakten über mehr als 500 Sicherheitsverletzungen auf, die über 4 Jahre hinweg gesammelt wurden. Das RISK-Team des Unternehmens fand dabei heraus, dass die Ursachen in 73 % aller Fälle externe Quellen sind.
Die größte Bedrohung für KMUs besteht in der Nachlässigkeit, nicht alle Windows-Patches im Veröffentlichungsmonat zu installieren. Da Ihr Netzwerk neben Microsoft-Produkten noch viele andere Programme enthält, muss die Patching-Routine systematisch auf alle Anwendungen und BS-Komponenten im Netzwerk ausgeweitet werden.

Maßnahme gegen automatisierte Angriffe

Investition in ein Patch-Management. Mit Hilfe von Patch-Management-Software können Sie Ihr Netzwerk auf fehlende Patches und Software-Updates prüfen bzw. die effektive Verteilung über eine zentrale Konsole sicherstellen. Dadurch gewährleisten Sie, dass Ihre gesamte Netzwerk-Software stets auf dem neuesten Stand ist.

Einrichten eines kostengünstigen Testnetzwerks. Selbst renommierte Unternehmen machen Fehler. Deshalb sollten Sie die Funktionalität von Patches vor der eigentlichen Implementierung auf einem Testsystem prüfen. Ein solches Netzwerk lässt sich kostengünstig mit ausgemusterten Computern und Servern einrichten.

Schlussfolgerung

Die vorgeschlagenen Abwehrmaßnahmen helfen zwar, Risiken zu verringern und die Netzwerksicherheit effektiv zu verbessern, abschließend ist diese Liste allerdings nicht. Weitere praktische Tipps zum Schutz Ihres Netzwerks gegen allgemeine Bedrohungen finden Sie im White Paper **Top Ten Security Threats for SMEs (and what to do about them)**, das Sie kostenlos von der WatchGuard-Website herunterladen können.

WatchGuard® bietet XTM (Extensible Threat Management) Gateway Security Appliances, die gegen neun der zehn hier aufgeführten Bedrohungen schützen. (Gegen das Verlieren von Hardware ist leider kein Kraut gewachsen.) Wir *können* Ihnen helfen, Ihr Wireless-Netzwerk zu schützen, die Integrität von Client-Zugriffsanforderungen auf Ihr Netzwerk zu

prüfen, Spam zu filtern, Web-Proxys einzurichten, Insider-Bedrohungen zu minimieren, VPNs zu erstellen und vieles mehr.

Weitere Infos zu WatchGuard-Sicherheitslösungen und wie Sie Ihr Netzwerk gegen Botnets und andere Netzwerkbedrohungen schützen können, erhalten Sie unter www.watchguard.de oder von Ihrem Händler.

©2008 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo, Firebox und LiveSecurity sind in den USA und/oder anderen Ländern entweder Markenzeichen oder eingetragene Markenzeichen von WatchGuard Technologies, Inc. Alle anderen Markenzeichen oder Markennamen sind Eigentum ihrer jeweiligen Besitzer. Teilenr. WGCE66599_112408