solarwinds msp

E-Book

7 Schutzmechanismen gegen Hacker

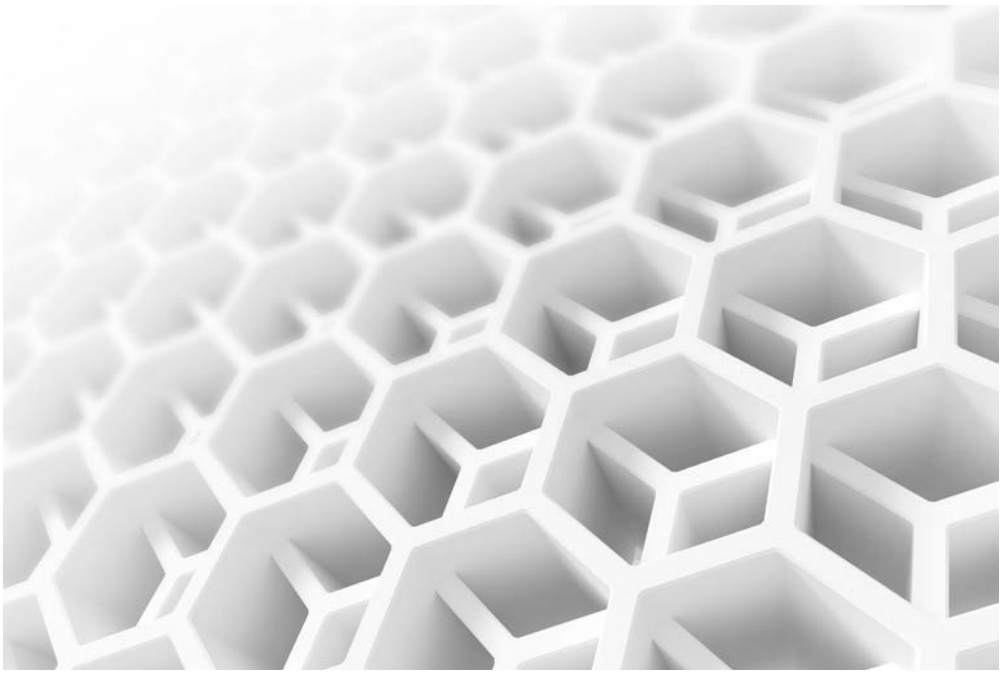
1. MEHRSTUFIGE SICHERHEITSMASSNAHMEN SIND EIN MUSS

SO GEWINNEN SIE DIE NÖTIGE ZEIT

Vielschichtige Sicherheit, mehrere Verteidigungslinien – wie auch immer das Konzept in Ihrem Unternehmen lautet, wichtig ist, dass Sie eine umfassende Schutzstrategie verwenden. Neu ist diese Erkenntnis nicht, aber heute mindestens genauso relevant wie in den Anfangsjahren des IT-Sicherheitsbewusstseins. Von zentraler Bedeutung ist natürlich die Wahl der richtigen Sicherheitsschichten. Stellen Sie sich eine umfassende Schutzstrategie einfach als Risikominderungsprogramm vor, das jeden Aspekt Ihrer IT-Infrastruktur durch mehrere Kontrollinstanzen oder -ebenen schützt.

Zwar kann auch die beste Strategie keinen 100-prozentigen Angriffsschutz gewährleisten, aber sie verlangsamt das Vordringen eines Hackereinbruchs und gibt Ihrem Unternehmen eine bessere Chance, sich vor Angriffen zu schützen. Mit einem gut aufgebauten mehrschichtigen Schutzkonzept gewinnen Sie Zeit, können wirksam gegen Angriffe vorgehen und das Risiko einer Sicherheitsverletzung mindern. Anders gesagt, machen Sie also Hackern das Leben schwer!

Und mit den folgenden 7 Maßnahmen können Sie dieses Ziel erreichen:



Neu ist diese Erkenntnis nicht, aber heute mindestens genauso relevant wie in den Anfangsjahren des IT-Sicherheitsbewusstseins.

2. PROAKTIVER SCHUTZ DURCH TRANSPARENZ IM NETZWERK

AUSSAGEKRÄFTIGE ANALYSEN FÜR ZIELGERICHTETE SICHERHEIT

Eine transparente Netzwerkinfrastruktur lässt Sie alles prüfen, alles erfassen, Anomalien erkennen und Richtlinien sinnvoll anwenden. Die Überwachung potenziell sicherheitsrelevanter Ereignisse ermöglicht aussagekräftige Analysen und damit den kosteneffizienten, proaktiven Schutz Ihrer Infrastruktur und Daten. Netzwerkvisibilität hilft, sich vor Angreifern zu schützen und deren Aktivitäten frühzeitig aufzudecken.

Einen gewissen Grad an Netzwerktransparenz erreichen Sie bereits mit kostenlosen Tools. OTX ThreatFinder von AlienVault gleicht beispielsweise Daten aus der Protokolldatei mit der Live-OTX-Datenbank ab, um infiltrierte Systeme und schädliche Inhalte zu identifizieren. Zu einer transparenten Netzwerkstrategie gehört aber auch zu wissen, was im Unternehmensnetzwerk vorgeht. Tripwire SecureScan ermöglicht die kostenfreie Prüfung von bis zu 100 IP-Adressen im Netzwerk, um verschollene und versteckte Geräte zu finden.

Vergessen Sie nicht: Je mehr Geräte im Netzwerk Internetzugang haben, desto höher ist das Risiko einer Kompromittierung.

3. BESSERER WEBSCHUTZ MIT RICHTLINIEN

HABEN SIE IHRE RICHTLINIEN FÜR DIE INTERNETNUTZUNG IM GRIFF?

Der Webschutz ist eine weitere wichtige Sicherheitsebene. Dieses Prinzip umfasst die Steuerung, Überwachung und Durchsetzung kundenspezifischer Richtlinien für die Internetnutzung über ein zentrales Front-End. Vereinfacht gesagt wird Ihre Infrastruktur durch Richtlinien geschützt. Mehrere Geräte können auf eine zentrale Richtlinie verweisen, die entsprechend bearbeitet und skaliert werden kann, damit keine Einstellungen auf Geräteebene vorgenommen werden müssen.

Sie können beispielsweise inhalts- und zeitbasierte Filter anwenden, Netzwerkengpässe mithilfe von Bandbreitenüberprüfung vermeiden und Ihr Unternehmen rechtlich absichern.

Vereinfacht gesagt wird Ihre Infrastruktur durch Richtlinien geschützt.

4. PATCH-MANAGEMENT ALS SICHERHEITSNETZ

KÖNNEN SIE MIT ANGREIFERN SCHRITT HALTEN?

Sie können den ganzen Tag lang nach Angriffsmustern suchen und jede denkbare Richtlinie anwenden, aber letztendlich kann kaum ein IT-Team mit der Schwemme an (fast täglich) neu auftauchenden Sicherheitsbedrohungen mithalten. Auch wenn das Patch-Management keine Wunderwaffe ist und nicht vor Zero-Day-Exploits schützt (vor allem nicht bei ungepatchten Systemen), ist es dennoch eine wichtige Maßnahme, um mit Hackern Schritt zu halten.

Es lohnt sich, Benachrichtigungen von Sicherheitsanbietern zu abonnieren, immer mal wieder einen Blick auf Sicherheits-News zu werfen und Patches einzuspielen, sobald dies sicherheitstechnisch empfehlenswert ist. Und genau darum geht es beim Patch-Management: Sie müssen nicht nur wissen, dass ein Patch verfügbar ist, sondern auch, dass er sicher installiert werden kann. Wird ein instabiler Patch ungetestet im Live-Betrieb implementiert, können die Folgen für das Geschäft im Ergebnis schädlicher sein als die Sicherheitslücke, die er schließen sollte.

5. WERTVOLLE DATEN MÜSSEN VERSCHLÜSSELT WERDEN

WELCHE DATEN SIND AM WICHTIGSTEN?

Das Problem der Datenverschlüsselung ist ihr Ruf: zu komplex, zu teuer, zu aufwändig. Dabei kann das Identifizieren und Verschlüsseln unternehmenskritischer Daten ganz unkompliziert ablaufen.

Sind Daten stark genug verschlüsselt, sind sie vor den meisten Hackern außerhalb des Verfassungsschutzes sicher. Und so einfach geht's:

- Tablets und Smartphones: Die im Betriebssystem integrierte Firmwareverschlüsselung macht diese Geräte für Unbefugte unbrauchbar. Vergessen Sie also nicht, dieses Feature zu aktivieren!
- Websites: Der HTTPS-Standard stellt sicher, dass Daten bei der Übertragung zwischen IT und Clientbrowsern verschlüsselt werden.
- Webbrowser: Mit HTTPS Everywhere werden Anforderungen von unverschlüsselten HTTP-Websites in sichere HTTPS-Seiten umgewandelt.
- USB-Sticks: Eine beliebte Verschlüsselungslösung im Open-Source-Format ist VeraCrypt. Dieses Programm ist kostenlos, anwenderfreundlich und hält, was es verspricht!

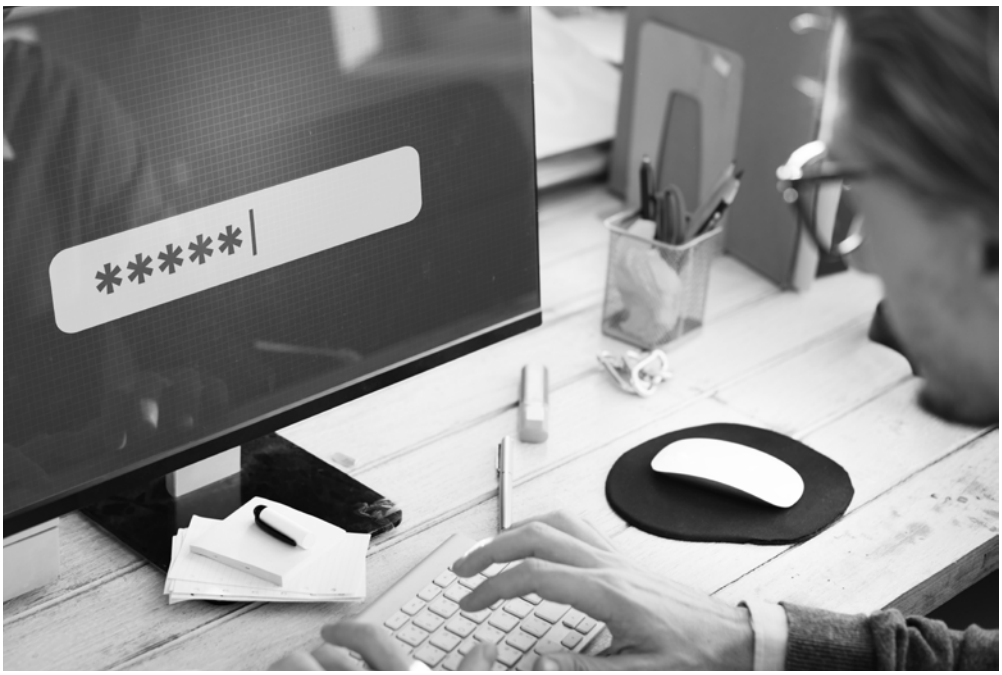
Sind Daten stark genug verschlüsselt, sind sie vor den meisten Hackern außerhalb des Verfassungsschutzes sicher.

6. DIE DEVISE LAUTET: AUTHENTIFIZIEREN, AUTHENTIFIZIEREN UND NOCHMAL AUTHENTIFIZIEREN!

VERWENDEN SIE AUSGEREIFTE AUTHENTIFIZIERUNGSRICHTLINIEN?

Die sichere Authentifizierung umfasst Passwortmanager und Mehrfaktorverfahren. Die Verwendung starker Kennwörter versteht sich von selbst. Leider lassen sich Kennwörter, die lang, komplex und willkürlich genug sind, um als sicher zu gelten, nur schwer merken. Und selbst Personen mit einem ausgesprochen guten Gedächtnis sind bei zu vielen Kennwörtern wohl überfordert. Genau da kommen Passwortmanager zum Tragen.

Eine entsprechende Lösung speziell für Unternehmen ist LastPass Enterprise – nicht kostenfrei, aber die Preisspanne beginnt bei unter 20 Euro pro Person. Mit diesem Tool können Sie Kennwortrichtlinien in der Cloud verwalten und im Handumdrehen wirklich sichere Kennwörter generieren. Doch auch das reicht noch nicht aus. Ein weiterer wichtiger Schritt ist die Multifaktor-Authentifizierung. Bei LastPass erfolgt die Zwei-Faktor-Authentifizierung (2FA) beispielsweise über ein Sicherheitstoken oder durch die Eingabe von Code, der mit einer App auf Ihrem Smartphone generiert wurde. Jede ausgereifte Authentifizierungsrichtlinie sollte mindestens die Zwei-Faktor-Authentifizierung verlangen.



7. FORENSISCH KORREKTES LÖSCHEN

WURDEN IHRE DATEN WIRKLICH SICHER VERNICHTET?

Als letzte Empfehlung auf unserer Liste mit Schutzebenen steht das sichere Löschen von Dateien. Diesen Aspekt lassen selbst Sicherheitsfanatiker oft außer Acht. Und wer kann es ihnen verdenken? Gelöschte Daten können keine Sicherheitsschwachstelle mehr darstellen, oder? Falsch gedacht! Gelöschte Daten sind nicht wirklich verschwunden (selbst nicht nach dem Formatieren der Festplatte). Eine Datenwiederherstellung ist nicht nur forensisch möglich, sondern sogar ganz einfach, schnell und kostengünstig. Ihre Aufgabe ist es, diese Prozedur so schwierig wie möglich zu machen. Wir empfehlen als Mindestschutz, Ihre Daten zu verschlüsseln und dann einzelne Dateien und Ordner mit einem Datenvernichtungsprogramm sicher zu löschen. Ein solches Tool ist zum Beispiel Eraser, das Festplattenbereiche in 35 Durchgängen mit Zufallsmustern überschreibt. Wenn das unwiderrufliche Löschen von Daten für Sie oberste Priorität hat, ist diese Software nicht das Nonplusultra. Aber sie ist kostenlos und in Verbindung mit einer Verschlüsselungsstrategie eine gute Lösung. Wer wirklich auf Nummer sicher gehen will, muss seine Festplatte wohl mit einem Metall-Shredder (gegen eine entsprechende Gebühr) mechanisch zerkleinern lassen.

Eine Datenwiederherstellung ist nicht nur forensisch möglich, sondern sogar ganz einfach, schnell und kostengünstig. Ihre Aufgabe ist es, diese Prozedur so schwierig wie möglich zu machen.