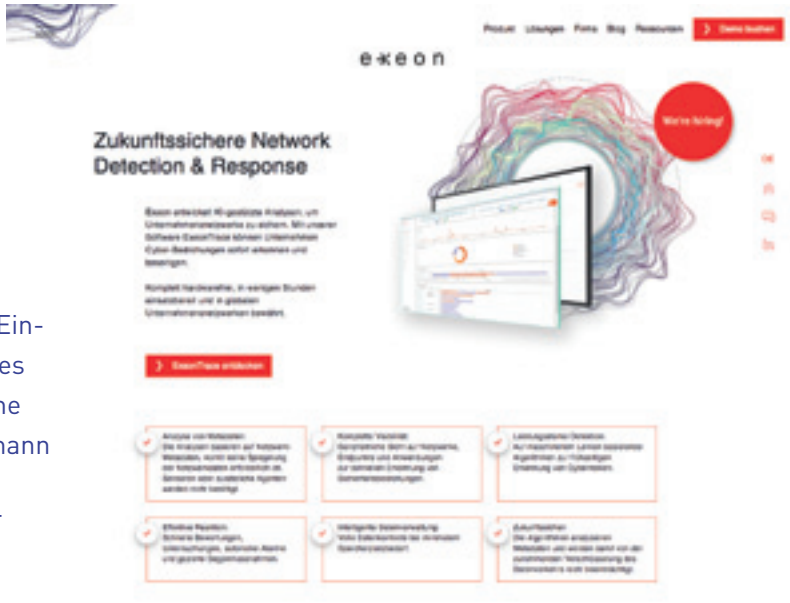
IT-Sicherheit **verbessern**



Größe und Bedeutung einer Institution haben keinen Einfluß darauf, wie gefährdet ihre IT ist. Potentiell ist jedes System bedroht – und umso wichtiger ist es, die eigene Infrastruktur bestmöglich abzusichern. David Gugelmann von Exeon Analytics mit Sitz in Zürich gibt 7 Tips, wie kleine und große Unternehmen die Sicherheit ihrer IT verbessern können ...

1. Entwickeln Sie ein Sicherheitsbewußtsein

Vor der Technologie kommt das Mindset. Das globale Netz existiert bereits seit drei Jahrzehnten und so gut wie kein Unternehmen kann – und will – ohne Anbindung an das Internet funktionieren. Das bedeutet auch, daß die Systeme von absolut jedem Unternehmen aus dem Netz heraus angegriffen werden können. Sich dessen bewußtzuwerden und eine zielgerichtete und ausgefeilte Verteidigungsstrategie zu erarbeiten und auszurollen, muß oberste Priorität haben – ganz gleich, in welcher Branche das Unternehmen tätig ist oder welche Größe es hat.

2. Evaluieren Sie die Risiken

Angesichts der zunehmenden Verlagerung in den digitalen Raum wird es immer schwieriger und auch kostspieliger, im Rahmen eines Sicherheitskonzeptes alle Unternehmensbereiche gleichwertig zu schützen. Es sollte genauestens evaluiert werden, welche Abteilungen für die reibungslose Abwicklung ihres Geschäfts absolut unabkömmlich sind. Diese bilden dann das Réduit eines Unternehmens, also ein spezieller Schutzbereich, für den die eigentliche Security-Strategie entwickelt werden muß – denn darin befindet sich die Grundlage der geschäftlichen Existenz.

3. Patchen ist die halbe Miete

Auch Software-Anbieter arbeiten nicht perfekt – doch sie versuchen zumindest, ihre Lösungen laufend zu verbessern. Insbesondere große Provider beschäftigen ganze Teams, die sich laufend darum kümmern, Fehler in einer Software aufzufinden und auszumerzen. Dazu zählen vor allem auch potentielle Sicherheitslecks oder andere Bugs, die Angreifern Einfallstore für Cyberattacken bieten können. Nicht selten schrecken Unternehmen davor zurück, diese Patches regelmäßig aufzuspielen – zu groß ist die Angst, im laufenden Betrieb Änderungen vorzunehmen, die potentiell für Ausfälle sorgen könnten. Oftmals fehlen auch schlicht die personellen oder finanziellen Ressourcen für ein IT-Team, das sich um diese Aufgabe kümmern könnte. Oft geht dieser Ansatz gut, doch je älter (und „ungepatchter") ein System ist, desto mehr Sicherheitslecks weist es auf, die in Hackerkreisen bekannt sind und von diesen ausgenutzt werden können. Zahlreiche Angriffe in der Vergangenheit waren genau aufgrund dieser Patchmüdigkeit erfolgreich und hätten durch laufende Aktualisierungen vermieden werden können.

4. Spielen Sie den Backup-Ernstfall durch

Für den Notfall ein Backup der wichtigsten Daten anzulegen, ist mittlerweile gängig und für die Datensicherheit sehr zielführend. Dennoch sollte ein wichtiger Aspekt rund um Backups nicht vergessen werden: Der Wiederherstellungsprozeß. Das IT-Team sollte gezielt in regelmäßigen Abständen versuchen, die Backup-Daten testweise auszurollen und die Systeme wieder zum Laufen zu bringen. Denn ist die IT im Ernstfall nicht in der Lage, die Systeme oder die Daten wiederherzustellen, nützt auch das beste Backup nichts– die wertvollen Daten sind dann entweder unbrauchbar oder gar zerstört.

5. Betreiben Sie in der Cloud strenges Identitätsmanagement

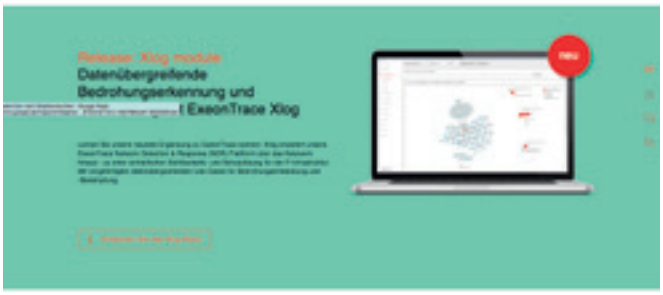
Cloud-Technologie ist längst ihren Kinderschuhen entwachsen, zahlreiche Firmen haben bereits ihre IT-Systeme in die „Wolke" ausgelagert oder mit dem Wechsel begonnen. Neben den zahlreichen wirtschaftlichen und prozessualen Vorteilen ergeben sich daraus auch einige Implikationen in Bezug auf die IT-Sicherheit. Gerade aufgrund der zahlreichen örtlichen Zugriffsmöglichkeiten auf kritische Daten ist es wichtig, das Identitätsmanagement für Cloud-Infrastrukturen genauestens unter die Lupe zu nehmen. Die Zugriffsrechte einzelner Benutzerkonten müssen strengstens reglementiert und definiert sein: Insbesondere die Zahl der Accounts, die viele Berechtigungen auf sich vereinen, muß möglichst gering sein. Mitarbeiter sollten nur über diejenigen Befugnisse verfügen, die sie unbedingt für die tägliche Arbeit benötigen.

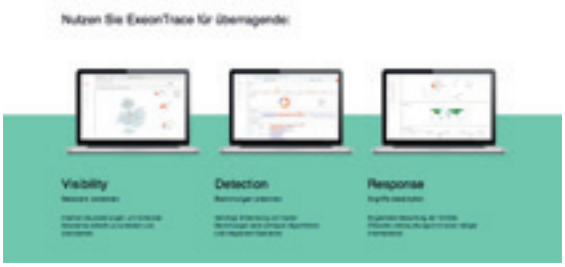
6. Lernen Sie Ihr Netzwerk kennen – bis in den letzten Winkel

Die IT-Infrastruktur von Unternehmen besteht nicht allein aus den offiziell betriebenen Systemen und Programmen. Gerade dort, wo die vorhandenen Applikationen nicht den eigenen Ansprüchen oder Ab-

Alle Bilder: Exeon Analytics

läufen genügen, entsteht sehr häufig eine sogenannte Schatten-IT. Dies bedeutet, daß sich Mitarbeiter mit Workarounds behelfen, wenn die ihnen zur Verfügung gestellten Mittel nicht geeignet und unzureichend sind, um ihre Aufgaben zu erfüllen. In der Folge etablieren sich Prozesse, die gerade dann nicht gut überwacht werden können, wenn nur eine Handvoll Angestellter überhaupt über sie Bescheid weiß. Idealerweise sollte das Wachstum dieser Schatten-IT folglich nicht nur allumfassend bekämpft werden, sondern auch – wo ihre Existenz möglicherweise sogar vonnöten ist – in das „offizielle" Monitoring mit eingebunden werden. Z.B. lassen sich private Laptops und Mobiltelefone nicht ohne Weiteres erfassen und in die Sicherheitsinfrastruktur einbinden – ebenfalls ein „ideales" Einfallstor für Eindringlinge.





7. Schließen Sie nicht nur die Lücken in Ihrer Firewall

Selbst die beste Firewall kann nicht gegen alle Angriffe schützen – zu komplex sind viele Systeme und es reicht ein einziges Schlupfloch, damit Angreifer ins System eindringen können. Hacker benötigen in aller Regel viel Zeit, um sich nach den wertvollsten Daten in einem System umzusehen. Genau in dieser Phase muß der Angriff erkannt und abgewehrt werden, um zu verhindern, daß Ihr Unternehmen Opfer eines Datendiebstahls oder der böswilligen Verschlüsselung ihrer IT-Systeme wird. Der Blick der IT muß sich deshalb auch nach innen richten – auf das Monitoring von Prozessen und die Beobachtung des eigenen Systems, denn nur so können verdächtige Aktivitäten früh genug erkannt und aufgespürt werden, bevor Schlimmeres passiert.

FAZIT

So, wie kein Haus vor Einbrechern hundertprozentig geschützt werden kann, gibt es auch kein IT-System, das vor Hackern absolut sicher ist. Das bedeutet jedoch nicht, daß man es potentiellen Eindringlingen leicht machen muß. Moderne Cybersicherheits-Ansätze gehen deshalb über die eigentliche Prävention hinaus und fokussieren die Detektion von Eindringlingen, um umgehend darauf reagieren zu können – analog einer Alarmanlage in einem Haus. Viele Angriffe der Vergangenheit hätten vermieden werden können, wären diese grundlegenden Punkte beachtet worden. <<

Noch Fragen? www.exeon.com