Security Service Update

Da Cyberkriminalität eine stetig wachsende Gefahr ist, die auch kleinere und mittlere Firmen angeht, machen wir allen unseren Kunden das Angebot, ihre IT Netzwerke mit einem hochwertigen IT Security Werkzeug auszustatten bzw. zu scannen.

Dieses Werkzeug bedeutet eine überprüfbare, dauerhafte Gewissheit, indem es Ihre IT-Infrastruktur aus Sicht eines Angreifers von außen, sowie von innen überprüft und uns mit einem praktischen Maßnahmenplan ausstattet.

Die Sicht eines Angreifers

Die Lösung zeigt bildlich dargestellt die offenen Fenster oder eine zu wenig gesicherte Eingangstür Ihres Gebäudes, durch die ein Angreifer eindringen könnte. Die monatlichen externen und täglichen internen Überprüfungen Ihres „Hauses" zeigen Ihnen immer den aktuellen Sicherheitsstand Ihrer IT und warnen Sie so vor neuen Bedrohungen und Einfallstoren.

Implementierung

A. Extern & Info zu intern

Zunächst prüfen wir monatlich Ihre externen Angriffsziele mit unserem neuen Security Audit Tool, um das Risiko eines Hacker-Angriffs einschätzen zu können. Wir erstellen einen Maßnahmenplan für Sie, um dieses Risiko zu minimieren und für die Zukunft vorbereitet zu sein.

Zusätzlich werden wir auch die internen Ziele überprüfen. Dafür werden wir einen Agenten auf Ihren Endgeräten installieren, der unmerklich im Hintergrund läuft und Ihre PCs und Server laufend auf Sicherheitslücken überprüft.

B. Extern & intern

Mit Implementierungsbeginn überprüfen wir automatisiert Ihre externe und interne Infrastruktur, um einen Überblick über die potenzielle Angriffsfläche zu gewinnen und das Risiko eines Hacker-Angriffs einschätzen zu können.

Fazit

Cyber-Kriminalität ist eines der größten vorherrschenden Gefahrenpotentiale, vor dem auch kleine und mittlere Unternehmen nicht bewahrt sind. In der heutigen Zeit ist es deswegen umso wichtiger auf ein automatisiertes und damit bezahlbares Tool zu setzen, das die dauerhafte Sicherheitslage eurer Infrastruktur zeigt und auswertet. Somit haben wir die Möglichkeit proaktiv zu handeln und potenziellen Angriffen entgegenzuwirken.

Zusammenfassung

01 Herausforderung

- KMUs geraten ins Fadenkreuz von Cyberkriminellen – als primäres Angriffsziel oder als Teil der Lieferkette von Großunternehmen.
- Zusätzlich wachsende Angriffsfläche aufgrund von automatisierten Angriffen, Digitalisierung, Homeoffice und steigender Komplexität der IT Infrastrukturen.
- Security-Dienstleistungen und bereits vorhandene Produkte sind für KMUs oft zu teuer.
- Standardprodukte wie z.B. Antivirus und Firewall bieten keine umfassende Sicherheit.
- Fehlende Transparenz der eigenen IT Sicherheitslage birgt Risiken.

02 Lösung

Produktbeschreibung
Für KMUs bietet Arbor-Link mit Lywand vollautomatisierte und kontinuierliche IT-Sicherheitsüberprüfungen Ihrer gesamten IT-Infrastruktur. Lywand schlägt Maßnahmen und Produkte vor, die die IT-Sicherheit messbar erhöhen.

Funktionen

- Bewertung der gesamten IT-Infrastruktur mithilfe von automatisierten Sicherheitsüberprüfungen.
- Bildliche und verständliche Darstellungen.
- Automatische Benachrichtigung bei einer Verschlechterung der Bewertung.
- Vorschläge von technischen und organisatorischen Maßnahmen.
- Automatisierte Priorisierung der Maßnahmen und Unterstützung bei der Umsetzung.
- Management Report mit den wichtigsten Informationen über Ihre IT-Sicherheitslage.

03 Vorteile

- Maßgeschneiderte Empfehlungen basierend auf Ihrer aktuellen Sicherheitslage.
- Unterstützung und Beratung von uns. Wir übernehmen die Planung und Umsetzung der Maßnahmen.
- Leistbare Preise ermöglichen auch Ihnen, Ihre IT-Sicherheit nachhaltig zu verbessern.
- Lywand schafft Ihnen Gewissheit und einen Überblick über Ihre Sicherheitslage.
- Ihre Sicherheitslage wird greifbar und messbar, und es ist kein blindes Vertrauen in ein Cybersecurity Produkt mehr nötig.

04 Produkt

Intern

- Intern werden die Ziele täglich überprüft, solange der Agent installiert ist.
- Ziele: Windows PCs (ab 7) und Windows Server (ab 2012 R2).

Extern

- 2 Scans
- Zusätzliche Scans können jederzeit durchgeführt werden.
- Ziele: (Sub-)Domains, IP-Adressen und E-Mail-Adressen.

Weitere Informationen unter: https://arbor-link.de/news/security-audit/