netfon

Sicherstellung Ihrer
IT-Security →

Firewall Up2Date

Cyber-Angriffe nehmen zu –
KMU verschlafen Sicherheitslücken!

Stunde für Stunde, am Tag oder in der Nacht – laufend werden neue Sicherheitslücken registriert: Gefahren, welche Ihr Schutzschild – die Firewall – kennen muss, um Sie effektiv davor schützen zu können.

Ausgangslage

Die MITRE Corporation, eine Organisation, die im Auftrag der USA diverse Forschungen durchführt, erhebt seit dem Jahre 1999 die weltweit anerkannte Liste «Common Vulnerabilities and Exposures» (CVE). Darin werden Sicherheitslücken und andere Schwachstellen in Computersystemen einheitlich erfasst und dokumentiert. Bewegte sich die Anzahl neu entdeckter Schwachstellen zu Beginn des 21. Jahrhunderts im tiefen vierstelligen Bereich je Jahr, so war der Wert der neu entdeckten Lücken seit 2017 nie geringer als durchschnittlich 1000 Neueinträge je Monat. Wir sprechen von einer neuen Sicherheitslücke pro Stunde. Wenige Tage bevor die neu entdeckten Schwachstellen für die Allgemeinheit zugänglich publiziert werden, erhalten die davon betroffenen Hersteller die Möglichkeit, das Problem mit einem Software-Patch zu beseitigen. Wurde die Sicherheitslücke erst einmal veröffentlicht, nimmt die Gefahr für die davon betroffenen Systeme massiv zu, da ab diesem Zeitpunkt auch bösartige Hacker über die Sicherheitslücke Bescheid wissen.

Wie kann ich mich schützen?

Wenn Sie ein Problem nicht kennen, heisst es nicht, dass es dieses nicht gibt – und es ist dann schwierig bis unmöglich, das Problem zu lösen. Schutz vor den neuesten Gefahren kann Ihre Firewall nur bieten, wenn sie diese kennt. Es ist essenziell, dass Ihr Tor zum Internet eine aktuelle Software verwendet, welche gegen möglichst viele potenzielle Angriffe gehärtet wurde. Damit dies der Fall ist, muss die Software in möglichst kurzen Abständen aktualisiert werden.

Wie können wir Sie unterstützen?

Als IT-Unternehmen verfolgen wir die Veränderungen am Markt genauestens – ob es sich im Positiven um neue Trends oder im Negativen um neue Bedrohungen handelt. Dadurch können wir abschätzen, zu welchen Zeitpunkten die Aktualisierungen durchgeführt werden sollen.

Ihre Vorteile

Zeit und Nerven sparen

Sie legen die Verantwortung für das regelmässige Aktualisieren Ihrer Firewall in unsere Hände. Wir planen die Aktualisierungen anhand der aktuellen Bedrohungslage, kümmern uns um allfällig notwendige Lizenzen und führen die Updates für Sie transparent durch.

Kalkulierbare Kosten

Sie erhalten Firewall Up2Date zum monatlichen Festpreis. Wir informieren Sie rechtzeitig über Produktabkündigungen (End of Life), welche Ihre Firewall betreffen.

Inbegriffene Leistungen

Konfigurations-Backups

Wir erstellen kontinuierlich automatische Konfigurations-Backups*1, mindestens zwei Konfigurations-Backups werden jährlich manuell durch einen Techniker durchgeführt. Dadurch kann z. B. bei einem Defekt das Gerät in kurzer Zeit anhand eines aktuellen Konfigurations-Backups wiederhergestellt werden.

Aktualisierung der Software

Wir planen und führen jährlich zwei Aktualisierungen der Firewall durch. Die Updates werden auf Basis der Bedrohungslage und bekannten Schwachstellen terminiert. Tendenziell werden die Aktualisierungen im Abstand von 4 bis 8 Monaten durchgeführt. Sie als Kunde werden rechtzeitig über anstehende Arbeiten und daraus resultierende Ausfälle informiert. Die Aktualisierungen werden für den Kunden transparent mit einem Protokoll dokumentiert. Allfällige notwendige Lizenzen sind im Preis inbegriffen.

Optionale Leistungen

All-inclusive Service-Level-Agreement SLA

Wir erstellen kontinuierlich automatische Konfigurations-Backups*1, mindestens zwei Konfigurations-Backups werden jährlich manuell durch einen Techniker durchgeführt. Dadurch kann z. B. bei einem Defekt das Gerät in kurzer Zeit anhand eines aktuellen Konfigurations-Backups wiederhergestellt werden. Allfällige notwendige Lizenzen sind im Preis inbegriffen.

Web-Inhaltsfilter*1

Der Web-Inhaltsfilter dient dazu, Webseiten auf deren Inhalt zu überprüfen und gegebenenfalls den Zugang dazu zu sperren. Gründe für eine Sperrung können anstössige oder illegale Inhalte sein. Häufig gesperrte Inhalte sind Pornografie oder Webseiten, welche Verherrlichung von Gewalt und Hass betreiben. Ebenfalls können als Virenschleudern bekannte Webseiten gesperrt werden. Der Web-Inhaltsfilter wird in kurzen Abständen aktualisiert und ist auf diese Weise tagesaktuell.

Die Verantwortung für den Internet-Anschluss und die damit konsumierten und veröffentlichten Informationen trägt der Abonnent des Anschlusses.

Anti-Virus*1

Das Modul Anti-Virus überprüft alle IP-Verbindungen auf Bedrohungen hin, die über die Firewall verlaufen. Pakete, die bekannte Viren enthalten, werden dadurch rechtzeitig identifiziert und bereits auf der Firewall verworfen. Die Funktion ist ein zusätzlicher Schutz zu Endpoint-Security-Produkten, welche sich auf den Arbeitsstationen befinden. Durchdass die Firewall mit einem anderen Anbieter von Viren-Signaturen zusammenarbeitet als Ihr Endpoint-Security Anbieter, verringert sich das Risiko eines Virenbefalls erheblich. Das Modul Anti-Virus wird in kurzen Abständen aktualisiert und kennt dadurch die neuesten Viren.

UTM*1

Unified Threat Management (UTM) enthält sowohl den Web-Inhaltsfilter als auch das Anti-Virus-Modul.

*1 Diese Leistung kann nur angeboten werden, wenn Sie vom eingesetzten Produkt unterstützt wird.

Fazit

Es ist wichtig, dass die Geschäftsleitung über die aktuellen Bedrohungen informiert ist. Entsprechend können konkrete Massnahmen ergriffen und auch umgesetzt werden.Mit der Betreuung Ihrer Firewall durch die Netfon Solutions AG und/oder einem Security Check können Schwachstellen aufgedeckt werden. Es empfiehlt sich, professionelle Unterstützung beizuziehen, um die Unternehmungssicherheit zielgerecht und nachhaltig zu sichern.

Kontakt

Andrea Cavegn
Teamleader
andrea.cavegn@netfon.ch
+41 44 497 11 77

Netfon Solutions AG
Höhenweg 2B, 8834 Schindellegi
www.netfon.ch
+41 43 888 00 22

IT-Sicherheit verlangt fundiertes Wissen

CISSP (Certified Information Systems Security Professional) ist ein Security-Zertifikat für IT-Profis. Es wurde vom (ISC)², auch als International Information Systems Security Certification Consortium bekannt, entwickelt. Das CISSP-Examen verlangt von den Absolventen alles ab. Dabei soll sichergestellt werden, dass sich eine für IT-Sicherheit in einem Unternehmen oder für einen Kunden zuständige Person entsprechendes Fachwissen angeeignet hat. Die Prüfung erfolgt in acht sogenannten Domains, auch CBK Domains (Common Body of Knowledge) genannt.

1. Security and Risk Management
2. Asset Security
3. Security Engineering
4. Communications and Network Security
5. Identity and Access Management (IAM)
6. Security Assessment and Testing
7. Security Operations
8. Software Development Security

Das CISSP-Zertifikat ist drei Jahre gültig. Danach muss das Fachwissen erneut unter Beweis gestellt werden. Profitieren Sie von der ausgewiesenen IT-Security-Kompetenz von Netfon Solutions AG.

← Andrea Cavegn, IT-Experte mit CISSP Zertifizierung, steht Ihnen für weitere Auskünfte gerne zur Verfügung.