IDARION
networking & security

Case Study

SCHILLER AG – RUNDUM-IT-SECURITY MIT FORTINET

NAHTLOS SICHER

Der wirksame Schutz von Daten, Applikationen und Portalen vor zerstörerischer Malware, vor unerlaubten Zugriffen und dreisten Attacken ist ein vielschichtiges Unterfangen – und erfordert ein nahtloses Zusammenspiel komplementärer Security-Lösungen, Systeme und Policies. Im Bestreben, ein Höchstmass an IT-Security zu erreichen, setzt die in Baar (ZG) domizilierte SCHILLER AG auf das nahtlose Zusammenspiel dedizierter Security-Appliances von Fortinet.

Nur wenige Firmen können für sich in Anspruch nehmen, nebst der globalen Präsenz auch im «Space» vertreten zu sein. Die weltweit tätige, in Baar domizilierte SCHILLER AG gehört dazu. Der führende Hersteller und Anbieter medizintechnischer Lösungen mit Schwerpunkt in der kardiopulmonalen Diagnostik (Herz- und Lungendiagnostik) und Therapie hat es mit ihrem Taschen-EKG-Gerät bis in den Weltraum beziehungsweise bis in die Raumstation ISS geschafft. Zum Lösungs- und Produktangebot des Anbieters medizinischer Spitzengeräte gehören Elektrokardiographen, Langzeit-EKG- und -Blutdruck-Rekorder, externe Defibrillatoren, Spirometer, Ergometer (inkl. kardiologische Rehabilitation), medizinische IT-Lösungen, Patientenüberwachungsgeräte und weitere Rettungsgeräte. Allesamt Lösungen, die Leben retten und Ärzte und Pflegepersonal in ihrer Arbeit unterstützen.

Das Einhalten höchster Sicherheitsstandards ist für SCHILLER eine Selbstverständlichkeit. Vor diesem Hintergrund erstaunt es nicht, dass das Medtech-Unternehmen auch im Bereich der IT-Security höchsten Ansprüchen verpflichtet ist. Dazu Martin Strickler, Leiter IT: «Um Daten, Applikationen und IT-Infrastrukturen vor Angriffen unterschiedlichster Art wirksam zu schützen, haben wir uns für die Umsetzung einer 360-Grad-

FORTINET

IT-Security-Strategie entschieden. Dabei setzen wir auf das umfassende Produktportfolio von Fortinet, dessen leistungsfähige Appliances alle denkbaren Anwendungsbereiche wie Firewalling, Access Control und Remote Access via SSL-VPN, E-Mail-Security, Web-Security und Secure WLAN unterstützen. Dank Fortinet profitieren wir von den Vorzügen dedizierter ‹best of breed›-Lösungen sowie von einer homogenen, einfach bedienbaren und nahtlos verknüpften Security-Infrastruktur.»

«TOTAL IT-SECURITY» – ALLES AUS EINER HAND

Auslösender Faktor zur Rundum-Erneuerung der IT-Security-Infrastruktur war die Neukonzeptionierung der firmenweiten Netzwerkinfrastruktur, für deren Planung, Umsetzung und Management die in Baar und Effretikon domizilierte Sidarion beauftragt wurde. Der unabhängige Systemintegrator ist fokussiert auf die Bereiche IT-Security, Networking, IP-Address-Management und konvergente Infrastrukturen.

Als Basis-Security-Plattform setzt SCHILLER auf einen FortiGate 800C Cluster. Die mit 10-Gbit-Ports bestückten, ASIC-beschleunigten Firewalls stellen alle relevanten Abwehr- und Sicherheitsmechanismen zur Verfügung – so etwa Stateful Inspection Firewalling, Application Control, WebFilter, Antivirus, Intrusion Prevention, SSL-Inspection und Traffic Shaping. Dank dem 7/24-Stunden-Subscription-Service FortiGuard werden die Firewalls kontinuierlich mit aktuellsten Signaturen versorgt und sind dadurch in der Lage, auch neueste Attacken zu erkennen und abzuwehren.

Nebst der Gewährung einer maximalen Gateway- und Netzwerk-Security ermöglichen die redundant eingebundenen Firewalls auch eine firmenspezifische Zonierung. So lassen sich Bereiche wie Entwicklung, Verkauf, Finanzen, HR und Systemmanagement sauber voneinander trennen. Strickler macht auf ein weiteres, für SCHILLER bedeutendes Leistungsmerkmal aufmerksam: der gesicherte Remote-Zugang ins Firmennetzwerk. «Die FortiGate-Appliances ermöglichen einen mittels SSL-VPN geschützten Zugang ins LAN. Dadurch ist es autorisierten Mitarbeitenden möglich, von zu Hause aus oder von unterwegs via Terminal-Server auf individuell freigegebene Daten zuzugreifen.» Strickler betont, dass der Remote Access auf sogenannten «Maschinenzertifikaten» basiert und folglich nur mit firmeneigenen, gemanagten Endgeräten möglich ist. Diese sind mit der Endpoint-Software FortiClient bestückt.

> «Dank Fortinet profitieren wir von den Vorzügen einer integralen, einheitlich gemanagten IT-Security-Gesamtlösung sowie von den Stärken einer ‹best of breed›-basierenden Architektur.»
>
> **MARTIN STRICKLER**
> **Leiter IT, Schiller AG**

UMFASSENDE E-MAIL-SECURITY

Dass SCHILLER auch im Bereich der E-Mail-Kommunikation nichts anbrennen lässt, wird durch die Einbindung der Secure Messaging Appliance FortiMail von Fortinet deutlich. Sie sorgt für einen umfassenden Viren- und Spyware-Schutz. Dazu beinhaltet sie fortschrittliche Spam-Erkennungs- und Filter-Methoden wie z. B. zugangsgerechte Filter, Content-Filter, globale und benutzerbezogene Black/White-List-Filter oder Spam Realtime Blackhole Lists (RBL). Eine kontinuierlich und automatisch aktualisierte IP-Reputations-Datenbank sorgt zudem dafür, dass Verbindungsanfragen von Absender-IP-Adressen mit schlechter Reputation gar nicht erst angenommen werden. Zudem stellt FortiMail mittels tiefgreifender Header-Analysen und dem Erkennen von Bildinhalten weitere Leistungsmerkmale für eine sichere E-Mail-Kommunikation zur Verfügung. Da keine hundertprozentige Garantie dafür besteht, dass nur schlechte E-Mails blockiert («false negative») und nur gute Nachrichten zugestellt werden («false positive»), bietet FortiMail eine sogenannte Quarantäne-Funktion. Sie speichert sämtliche abgewiesenen Nachrichten in einem eigenen Bereich und stellt diese für einen späteren Abruf durch die jeweiligen User zur Verfügung. Somit gehen keine fälschlicherweise nicht zugestellten Nachrichten verloren.

GESICHERTE WEB-PORTALE

Ein weiterer sicherheitsrelevanter Themenbereich ist laut Strickler die elektronische Kommunikation mit Tochtergesellschaften, Mitarbeitenden, Distributoren und Kunden sowie der elektronische Austausch von Daten und Informationen. Dazu betreibt SCHILLER ein auf SharePoint 2013 basierendes Extranet/Intranet. Dass auch bei Diensten, die via Internet erreichbar sind, keine Abstriche bezüglich Sicherheit gemacht werden müssen, dafür sorgt die bei SCHILLER installierte «Web Application Firewall» FortiWeb 400C von Fortinet. Die als «Reverse Proxy» eingebundene Plattform beinhaltet sämtliche Security-Features, die zur umfassenden Absicherung von Web-Applikationen notwendig sind und weiss Angriffsmethoden wie SQL Injection, Cross Site Scripting, Buffer Overflow und Brute Force Login zu parieren.

Die mittels URL-basierter Policies konfigurierte FortiWeb-Appliance sorgt dafür, dass Web-Applikationen nicht lahmgelegt werden können, dass keine nicht autorisierten Personen auf sensitive Informationen in Datenbanken zugreifen und dass Webseiten nicht kompromittiert werden können. Dazu verhindert sie das Austauschen oder das Modifizieren von Applikationsdateien durch Dritte (Defacement), beinhaltet eine

kontinuierliche HTTP-RFC-Compliance-Prüfung, schützt vor Datendiebstahl und dem Auslesen von Applikations-Parametern und erkennt Schwachstellen der geschützten Anwendungen (Vulnerability Scanning). Ebenso wertvoll sind Leistungsmerkmale wie das dynamische und automatische Sperren von IP-Adressen mit schlechter Reputation, GEO IP Filtering sowie die Steigerung der Performance mittels Layer 7 Load Balancing, XML Routing und SSL/TLS Encryption.

SICHERE USER-AUTHENTISIERUNG

Um ausgewählten Usern via VPN-Gateway einen gesicherten Remote-Zugang ins Firmennetz zu ermöglichen – beispielsweise für das regelmässige Finanz-Reporting der einzelnen Niederlassungen oder für Mitarbeitende im Aussendienst – setzt SCHILLER auf ein umfassendes User Identity Management bzw. auf ein intelligentes Login-Verfahren («Strong Authentication»). Dazu Martin Strickler: «Auch in diesem Themenbereich sind wir mit Fortinet perfekt bedient. So stellt der Security-Spezialist mit FortiAuthenticator eine zentrale Instanz für eine sichere User-Authentifizierung (Überprüfung der Echtheit der berechtigten Person) und User-Autorisierung (Freigabe von Anwendungen gemäss individuell vergebenen Rechten) zur Verfügung. Sie basiert auf der sogenannten 2-Faktor-Authentifizierung, bei der User-Name und Passwort durch ein zeitbasierendes Einmalpasswort (OTP) ergänzt werden.»
FortiAuthenticator unterstützt wahlweise Hardware-, Mobile-, SMS- und E-Mail-OTP-Token, wobei bei SCHILLER primär die App-basierte Lösung «FortiToken Mobile» im Einsatz ist. Diese macht Smartphones und Tablets (iOS, Android) zum mobilen OTP-Token bzw. zum persönlichen Authentifizierungs-Device, besticht durch ein einfaches Rollout und eine komfortable Lizenz-Aktivierung. Für User ohne Smartphone unterstützt FortiAuthenticator die Übertragung des One Time Passwords als SMS. Zudem lässt sich das OTP auch als E-Mail-Nachricht übermitteln.
Dank der Unterstützung von LDAP und RADIUS sowie der nahtlosen Active-Directory-Einbindung erweist sich die FortiAuthenticator-Einbindung in bestehende IT-Landschaften als ausgesprochen schnell und komfortabel.

> «Know-how, Erfahrung und Engagement unseres IT-Partners Sidarion sind einzigartig. Er hält uns mit hochkarätigen Managed Services den Rücken frei.»
>
> **MARTIN STRICKLER**
> Leiter IT, Schiller AG

INTEGRALE SECURE-WLAN-LÖSUNG

In Ergänzung zu den bereits umgesetzten Massnahmen zur Maximierung der IT-Security plant SCHILLER den Aufbau einer sicheren WLAN-Infrastruktur. «Auch in diesem Bereich setzen wir auf Fortinet und profitieren einmal mehr von der nahtlosen Durchgängigkeit des ganzheitlichen IT-Security-Lösungsangebots», äussert sich Strickler zur anstehenden Beschaffung. Und er ergänzt: «Access Points, Firewall und Controller bilden bei Fortinet eine integrale Gesamtlösung. Sie basiert auf den bereits installierten FortiGate 800C Appliances, welche die performanten WLAN-Controller-Funktionen bereits beinhalten. Dadurch wird es möglich, den gesamten Datenverkehr der verteilten APs (Access Points) über die zentrale Security-Appliance zu leiten. Dies hat zur Folge, dass der WLAN-basierten Kommunikation alle bestehenden Abwehr- und Sicherheitsmechanismen zur Verfügung stehen. Dadurch erreicht das Funknetz denselben hohen Security-Level wie das kabelgebundene LAN.»
Die integrale Secure-WLAN-Lösung von Fortinet bietet ein zentrales Management sämtlicher APs und der damit verbundenen «Next Generation Firewall»-Sicherheitsfunktionen. Zudem ermöglicht sie die Bildung und Trennung unterschiedlicher virtueller Netze. Folglich lassen sich mittels derselben physischen APs mehrere unterschiedliche Wireless-Netzwerke mit individuellen Security-Policies betreiben. Für Strickler ein weiteres Argument, das für den Aufbau einer Fortinet-basierten WLAN-Infrastruktur spricht.

SIDARION
networking & security

SCHILLER

Die weltweit tätige SCHILLER AG zählt zu den führenden Unternehmen bei Entwicklung, Produktion und Vertrieb von medizinischen Geräten für die kardiopulmonale Diagnostik, die Patientenüberwachung sowie die Notfallmedizin. Bekannt geworden ist SCHILLER namentlich für seine Taschen-EKG-Geräte und -Defibrillatoren, die überall auf der Welt und sogar im Weltraum (ISS) Leben retten. Zum Angebotsumfang gehören Elektrokardiographen, Langzeit-EKG- und -Blutdruck-Rekorder, externe Defibrillatoren, Spirometer, medizinische IT-Lösungen und Patientenüberwachungsgeräte. Das 1974 gegründete, inhabergeführte und finanziell unabhängige Unternehmen beschäftigt beinahe 1000 Mitarbeitende (davon rund 200 im Headquarter in der Schweiz), verfügt über 30 Tochtergesellschaften und über 100 weitere Vertretungen weltweit.

SIDARION

Die 2003 gegründete, in Baar (ZG) und Effretikon (ZH) domizilierte Sidarion AG zählt zu den etablierten Lösungsanbietern in den Bereichen IT-Security, IP-Address-Management, Networking, Netzwerk-Überwachung und konvergente Infrastrukturen. Das Team topausgebildeter und erfahrener Spezialisten sorgt für umfassende Dienstleistungen. Diese reichen von der Beratung und Konzeptionierung über die Planung und Implementierung bis hin zu Wartung und Support komplexer Umgebungen. Zu den Kunden von Sidarion zählen namentlich mittlere und grosse Unternehmen in der Schweiz sowie international tätige Unternehmen mit Hauptsitz in der Schweiz.

SIDARION AG
Lättichstrasse 6
CH-6340 Baar

Rikonerstrasse 21
CH-8307 Effretikon

Tel.: +41 43 544 10 66
www.sidarion.ch