

GATEWAY-SECURITY MIT XTM-APPLIANCES VON WATCHGUARD

Air Zermatt – wenn Sekunden zählen

Im Bestreben, Applikationen und ICT-Infrastruktur vor Malware und Angriffen wirksam zu schützen, setzt Air Zermatt auf XTM-Appliances von WatchGuard – und auf Security-Services aus der Schweizer Cloud des «Managed Security Service Providers» (MSSP) Seabix AG.

Opportunitätskosten sind Kosten, die ganz schön ins Geld gehen können. Diese Erfahrung hat die im Oberwallis tätige Air Zermatt gemacht. Das Helikopter-Unternehmen, das mit seinen rund 65 Mitarbeitenden und neun Helikoptern sowohl Rettungseinsätze als auch Transport-, Touristen- und Taxiflüge anbietet, setzt im Bereich der ICT-Infrastruktur auf einen klassischen (reaktiven) «on premise»-Ansatz. Dabei bezog das Unternehmen in der Vergangenheit Produkte und Lösungen von verschiedenen IT- und Kommunikationsanbietern, was zu einer heterogenen, wenig flexiblen und folglich teuren ICT-Infrastruktur sowie zu unnötigen Schnittstellen führte. Wichtiger noch: Der Systemunterhalt und der User-Support erfolgten durch interne Mitarbeitende der Air Zermatt im Nebenjob. Dies mit der Konsequenz, dass diese nicht mehr genügend Zeit für ihre eigentlichen Aufgaben hatten.

Vor diesem Hintergrund entschied die Geschäftsleitung, die ICT auf ein neues Fundament zu stellen. In diesem Bestreben fündig geworden ist das Unternehmen beim Swisscom-Partner Seabix AG, einem ICT-Outsourcing-Dienstleister (Full Outsourcing), der sämtliche Bereiche der Informations- und Kommunikationstechnologie mittels standardisierter, flexibel anpassbarer Module abdeckt. Dazu gehören einerseits vor Ort installierte Komponenten und Systeme wie Netzwerk, Telefonie und Workspace – andererseits (Datacenter-)Services aus der Schweizer Cloud wie virtualisierte Server, Datenablage und Datensicherheit oder Mail-Services.

IT-Security – dreifach wirksam

Um die ICT-Infrastruktur bereits am Perimeter zu schützen beziehungsweise die vielfältigen Gefahren am Firmengateway abzuwehren, setzt Seabix auf XTM-Security-Appliances von WatchGuard. Dabei handelt es sich um leistungsfähige



Die Air Zermatt AG ist ein unverzichtbarer Dienstleister in den Bereichen (alpine) Rettung und Transport. (Bild: Air Zermatt)

Beteiligte Firmen

- Kunde:
Air Zermatt AG
(www.air-zermatt.ch)
- Reseller/Service-Provider:
Seabix AG
(www.seabix.com)
- Distributor:
BOLL Engineering AG
(www.boll.ch)



WatchGuard – Gefahren wirksam begegnen

IT-Security-Gesamtlösung mit beeindruckenden Leistungsmerkmalen (nicht abschliessend):

- XTM-Security-Appliances vereinen sämtliche relevanten IT-Security-Funktionen in einer hoch performanten Hardware (inkl. Application Control, URL-Filter, Antispam, Antivirus, Intrusion Prevention, SSL-VPN etc.)
- Maximaler Gateway- bzw. Perimeterschutz
- Umfassende und individuell wählbare Sicherheitsservices auf Abo-Basis
- Visualisierungs- und Reportingtool WatchGuard Dimension verdichtet alle sicherheitsrelevanten Informationen und macht diese in konsolidierter, verständlicher Form sichtbar

Plattformen, die sämtliche relevanten Sicherheitsfunktionen in einem System vereinen. Dazu gehören unter anderem Statefull Inspection Firewall, Malware Detection, Application Control, URL-Filter, Antivirus, Intrusion Prevention, SSL-VPN und Traffic Shaping. Dank der Konsolidierung dieser und weiterer Funktionen schützen die performanten Systeme den gesamten ein- und ausgehenden Datenverkehr verzögerungsfrei in Echtzeit – selbst bei höchsten Bandbreiten. Beachtenswert ist ferner, dass die WatchGuard-Appliances die zeitgleiche Einbindung mehrerer Access-Lines ermöglichen. In diesem Zusammenhang von besonderer Bedeutung sind Funktionen wie Lastverteilung (Load Balancing) und «Policy-based Routing».

«**Bezahlbare» Security**

Dass sich die Air Zermatt auf eine jederzeit massgeschneiderte und wirksame IT-Security verlassen kann – dafür sorgt Seabix mit ihrem «MSSP»-Programm, das sie als autorisierter WatchGuard-MSSP-Partner (Managed Security Service Provider) anbieten kann. Dabei handelt es sich um ein modulares beziehungsweise durch den Kunden frei wählbares Dienstleistungsangebot, das Services wie Wartung und Support, Lizenzen für aktivierte XTM-Funktionen, Software-Updates und Malware-Signatur-Update-Services beinhaltet. Dazu Thierry Kramis, Gründer und CEO von Seabix: «Dank unseres WatchGuard-MSSP-Status sind wir in der Lage, unseren Kunden exakt die Leistungen und XTM-Funktionen zur Verfügung zu stellen, die sie tatsächlich benötigen. Wichtig ist dabei, dass sich der Service auf monatlicher Basis den neuen Bedürfnissen und Bedrohungslagen anpassen lässt. Das modulare Servicemodell, das sich auch durch transparente Kosten auszeichnet, trägt aus unserer Erfahrung dazu bei, dass kurzfristige finanzielle Überlegungen nicht mehr auf Kosten der Security gehen.»



AUTOR
Jürg Hefel
 ist Product Manager WatchGuard bei BOLL in Wettingen (www.boll.ch)



«**Mit WatchGuard und Seabix AG setzen wir auf eine massgeschneiderte IT-Security-Gesamtlösung und profitieren von einem umfassenden Perimeterschutz.**»

André Zenhäusern, Air Zermatt AG

Security-Appliances von WatchGuard schaffen maximalen Gatewayschutz
 (Bild: WatchGuard)

Als weiteren Schlüsselfaktor nennt Kramis das einfache Rollout der XTM-Appliances sowie die komfortable Bedienung derselben. «Hinsichtlich Usability setzen die Systeme von WatchGuard einen klaren Standard. Sie sind derart intuitiv zu bedienen, dass deren Konfiguration, das Abbilden von Security-Policies sowie das Anpassen an neue Gegebenheiten einfach und schnell von der Hand gehen. Zudem steht uns mit «RapidDeploy» ein cloud-basierender Service zur Verfügung, der die komplett automatische Konfiguration neuer und verteilter XTM-Appliances ermöglicht. So etabliert die durch uns vorkonfigurierte Box beim initialen Setup eine gesicherte Verbindung mit dem Seabix-Datacenter, wird dabei von RapidDeploy erkannt und automatisch konfiguriert.» Kramis ergänzt, dass sich sämtliche installierten Appliances im Betrieb zentral über das Datacenter managen lassen. «Dadurch können sie bei neu auftretenden Gefahren umgehend angepasst werden und Sicherheitslücken lassen sich zeitnah schließen.»

IT-Security sichtbar machen

XTM-Appliances überwachen und analysieren stetig den gesamten Netzwerkverkehr und generieren dabei enorme Datenmengen. Damit der Überblick im Datenschwungel nicht verloren geht, sind Big-Data-Visualisierungswerkzeuge notwendig. Diese verdichten die aggregierten (Protokoll-)Daten in ver-

wertbare Sicherheitsinformationen und machen das sicherheitsrelevante Geschehen im Netzwerk und am Gateway einfach verständlich sichtbar. Dadurch unterstützen sie Security-Verantwortliche beim sofortigen Erkennen sicherheitsbezogener Vorkommnisse und Gefahren.

Eine beeindruckende Visualisierungs- und Reportinglösung stellt WatchGuard für ihre XTM-Security-Appliances zur Verfügung. Dazu Kramis: «Mit den Visualisierungslösungen von WatchGuard bieten wir den Kunden einzigartige Services zur Maximierung der Netzwerksicherheit an. Durch die Kombination aus Big-Data-Visualisierung und Reporting können wir wichtige sicherheitsrelevante Probleme und Trends zeitnah erfassen, eingrenzen und reporten. So ist es uns beispielsweise möglich, zu veranschaulichen, welche Webseiten und Kategorien von internen Usern am häufigsten aufgerufen und welche Applikationen genutzt werden, ob vertrauliche Daten das Unternehmen verlassen, welche kritischen Aktivitäten von internen Benutzern ausgeführt werden, welche Nutzer und Anwendungen besonders viel Bandbreite benötigen oder wo konkrete Angriffe stattfinden und aus welchen geografischen Regionen diese stammen. Informationen dieser Art unterstützen uns einerseits bei der Definition zielgerichteter Security-Policies – andererseits bei der zeitnahen Umsetzung geeigneter Massnahmen zur Anpassung an sich verän-

dernde Bedrohungslagen. WatchGuard Dimension stellt uns mittels Executive Dashboard modernste und einfach verständliche Visualisierungsformen zur Verfügung. So zum Beispiel Kacheldiagramme, die mit unterschiedlich grossen Flächen die Aufmerksamkeit der Betrachter sofort auf die Hotspots des Geschehens richten. Dadurch lässt sich schnell erfassen, was wo passiert und wo unmittelbarer Handlungsbedarf besteht.»

André Zenhäusern von der Air Zermatt ergänzt: Der mittels Visualisierungs- und Reportingplattform gewährte Einblick in die Kundeninfrastruktur durch unseren Partner Seabix ist insbesondere im Supportfall von entscheidender Bedeutung. Mit WatchGuard und den weitreichenden Services von Seabix sind wir auch im Bereich der IT-Security auf der sicheren Seite.»



BOLL ENGINEERING AG

Jurastrasse 58
 5430 Wettingen
 Tel. 056 437 60 60
 info@boll.ch, www.boll.ch