VIER WALDSTÄTTERSEE

BOLL IT Security Distribution

MIT FORTINET AUF DER SICHEREN SEITE – UMFASSENDER PERIMETER-SCHUTZ FÜR DIE SGV

Die Schifffahrtsgesellschaft des Vierwaldstättersees (SGV) AG setzt auf UTM-Appliances von Fortinet. Die integrale Gesamtlösung bietet ein Höchstmass an Sicherheit, Performance und Verfügbarkeit.

FORTINET

Attraktiver könnte die Domain www.lakelucerne.ch nicht sein. Sie steht für Freizeit und Genuss, für Erlebnis und Erholung. Dass sich internationale Touristen, Schulklassen, Tagesausflügler und Business-Leute im Herzen der Schweiz gleichermassen wohlfühlen, dafür sorgt zu grossen Teilen die Schifffahrtsgesellschaft des Vierwaldstättersees (SGV). Ältester Bereich ihres weitreichenden Dienstleistungsangebots ist die Schifffahrt. Das seit mehr als 175 Jahren mit dem Vierwaldstättersee verbundene Unternehmen besitzt eine der grössten Binnensee-Dampferflotten der Welt und sorgt mit nicht weniger als 22 Passagierschiffen unterschiedlichster Grösse und Bauart sowie einer Panorama-Yacht für touristische Höhepunkte.

Ebenso bedeutsam wie die Schifffahrt sind die beiden zur SGV-Gruppe gehörenden Unternehmen Shiptec und Tavolago. Shiptec bietet umfassende Dienstleistungen in der Entwicklung, in Bau und Instandhaltung von Fahrgastschiffen, Arbeitsschiffen und Yachten. Nebst der SGV selbst setzen zahlreiche weitere lokale und internationale Kunden auf die jahrzehntelange Erfahrung des Branchenprimus Shiptec.

Die Tavolago AG ist der «kulinarische Arm» der Firmengruppe. Sie kümmert sich um das leibliche Wohl der Gäste auf den Schiffen sowie in den bei diversen Häfen betriebenen Bistros.

Auch als Caterer für Geschäfts- und Privatkunden sowie als fester Gastronomiepartner für bedeutende Kunden wie Swiss Life Arena und Messe Luzern hat sich das Unternehmen einen Namen gemacht.
Heute erwirtschaftet die SGV-Gruppe einen Jahresumsatz von über 60 Millionen Franken, beschäftigt rund 450 festangestellte Mitarbeitende und zählt während der Hauptsaison (Sommer) bis zu 600 Mitarbeiterinnen und Mitarbeiter.

> «Die UTM-Appliances von Fortinet verbinden Sicherheit, Performance und Funktionalität auf überzeugende Weise.»
>
> **RICO ZEMP**
> Systemadministrator und Security-Verantwortlicher, SGV

KOMPLEXE IT FÜR EINEN REIBUNGSLOSEN BETRIEB

Um langfristig auf eine performante, sichere und stets verfügbare Informations- und Kommunikationstechnologie zählen zu können, hat sich die SGV-Gruppe entschieden, die über die Jahre organisch gewachsene IT-Infrastruktur zu erneuern. Dank diesem, gemeinsam mit dem IT-Partner Leuchter IT Infrastructure Solutions umgesetzten Migrationsprojekt erfreut sich die SGV heute einer komplett virtualisierten Infrastruktur. Deren Kern bilden zwei redundant aufgebaute, geografisch verteilte Rechenzentren, die via Glasfaser (iSCSI) miteinander verbunden sind. Über 32 virtuelle Server sowie mehrere Storage Systeme sorgen dafür, dass die rund 250 Clients und 50 virtuellen Desktops jederzeit einen performanten Zugriff auf Applikationen und Daten erhalten.
Laut Rico Zemp, Mitglied des vierköpfigen IT-Teams der SGV und für die Belange der IT-Security zuständig, bot die Erneuerung der Firmen-IT eine ideale Gelegenheit, auch die Informatiksicherheit auf ein neues Fundament zu stellen. «Unser konstantes Wachstum, die dezentrale Firmenstruktur sowie das vermehrte Aufkommen intelligenter Angriffsmethoden und ‹Modern Malware› führte dazu, dass unsere in die Jahre gekommenen Firewalls nicht mehr allen Gefahren gewachsen waren. Es wurde Zeit, neue Systeme zu evaluieren, die uns einerseits einen umfassenden Perimeterschutz gewährleisten und andererseits unsere Sicherheitsbedürfnisse im mobilen Bereich umfassend abdecken.»

UTM-APPLIANCES SCHAFFEN INTEGRALE SICHERHEIT

Aufgrund der veränderten Bedürfnisse hat sich Zemp mit seinem Team an die Evaluation einer neuen Gateway-Security-Infrastruktur gemacht und sich dabei für UTM-Appliances der FortiGate-Familie von Fortinet entschieden. Diese beinhalten sämtliche relevanten «Unified Threat Management»-Funktionen zur Sicherung des gesamten Netzwerkverkehrs in einem System. Dazu gehören Leistungsmerkmale wie Firewalling, Antivirus, VPN und SSL-VPN ebenso wie Anwendungskontrolle, Intrusion Prevention und Web-Filtering. Die Einbindung unterschiedlicher Security-Features in einer leistungsfähigen Appliance macht aus vielerlei Gründen Sinn. Zum einen wird die nahtlose Überwachung des gesamten Netzwerkverkehrs auf hoher Ebene möglich. Zum anderen reduziert sich die Zahl der benötigten Hardware- und Software-Komponenten markant, was sowohl die Beschaffungs- als auch die Lizenz- und Unterhaltskosten minimiert. Bedeutsam ist laut Zemp zudem die Möglichkeit, einzelne Security-Funktionen selektiv zu aktivieren bzw. zu nutzen. «Gewisse in der Vergangenheit installierte ‹Best of breed›-Lösungen haben wir nach wie vor in Betrieb. IPS beispielsweise haben wir auf den FortiGate-Appliances noch nicht aktiviert, können dies aber zum gegebenen Zeitpunkt tun. Ebenso verhält es sich mit Application-Control, die von der Appliance zwar unterstützt, von uns jedoch noch nicht genutzt wird. Sie steht uns jederzeit ohne Investitionen in zusätzliche Hardware oder Software zur Verfügung. Dank den UTM-Appliances von Fortinet erhalten wir ein hohes Mass an Flexibilität und Investitionsschutz.»
Dass der Entscheid zugunsten von Fortinet ausfiel, hat laut Zemp viele Gründe: «Einerseits überzeugen die FortiGate-UTM-Appliances durch ein ausgesprochen attraktives Preis-Leistungs-Verhältnis. Andererseits adressieren sie sowohl die Bedürfnisse von KMU als auch die Leistungsanforderungen von Grossfirmen. In unseren Datacentern beispielsweise ist ein Fortinet-Cluster mit Enterprise-tauglichen Systemen im Einsatz. Demgegenüber verwenden wir in den einzelnen Aussenstellen sowie auf den Schiffen FortiGate-Appliances der Small-Business-Klasse. Den unterschiedlichen Modellen zum Trotz: Wir profitieren von einem integralen Systemmanagement, einem

DIE MULTI-THREAT SECURITY-APPLIANCES DER FORTIGATE-FAMILIE VON FORTINET ÜBERZEUGEN AUF DER GANZEN LINIE:

- **Hoch performante UTM Appliance**
- **Beinhaltet sämtliche heute denkbaren Abwehr- und Sicherheitsmechanismen. So etwa Statefull Inspection Firewalling, Application Control, WebFilter, Antivirus, Intrusion Prevention und SSL Traffic Inspection**
- **Maximierte Performance dank ASIC-basierten Beschleunigungskarten**
- **Virtualisierte Ports (VLAN), getrennte Domains (VDOM) und mehrere virtualisierte Firewall-Instanzen**
- **High Availability dank Features wie Cluster-Installationen, geografische Redundanz und unterbruchsfreie Upgrades**

über alle Plattformen hinweg identischen GUI und einer komfortablen Einbindung von User- und Device-spezifischen Security-Policies.»

POSITIVE ERFAHRUNGEN AUF ALLEN EBENEN

Der konsolidierte UTM-Ansatz mit systemübergreifenden Konfigurations-, Analyse- und Kontrollfunktionen bildet laut Zemp eine wesentliche Voraussetzung, um modernen Gefahren wirksam zu begegnen. «Unsere Schiffe beispielsweise sind allesamt via UMTS mit dem Firmennetzwerk und folglich mit Daten und Anwendungen verbunden. Um dabei eine maximale Sicherheit zu gewährleisten, erfolgt die Datenkommunikation zu den UTM-Appliances im Datacenter via gesicherter VPN-Tunnels. Doch diese Vorkehrung alleine reicht nicht aus. Wir wollen auch sicherstellen, dass nicht auf kritische Websites zugegriffen wird und sich dadurch die Gefahr für unser Firmennetz unnötig erhöht. Deshalb machen wir uns den integralen URL-Filter zunutze. Dieser ermöglicht die Definition sogenannter ‹White Lists› beziehungsweise die Festlegung zugelassener URLs. Dabei sind alle nicht explizit erwähnten Domains für die User gesperrt. In diesem Zusammenhang sicherheitsrelevant ist ferner der in jeder UTM-Appliance integrierte Web-Filter. Dieser erlaubt an den einzelnen Standorten ausgewählte Websites oder Website-Kategorien zu sperren, den Zugang zu beschränken und Aufrufe zu loggen.»

Von grosser Wichtigkeit ist für die SGV ferner die Funktion FortiClient. Diese erlaubt den einfachen Aufbau SSL-verschlüsselter VPN-Tunnels (SSL VPN) und folglich die gesicherte Einbindung mobiler User- und Heim-Arbeitsplätze ins Firmennetzwerk. Voraussetzung dazu ist lediglich die Installation eines schlanken FortiGate-Software-Clients auf den berechtigten mobilen Devices (z. B. Notebook) sowie die Ausstellung eines User-bezogenen Zertifikats.

> «Dank der intensiven Zusammenarbeit mit unserem IT-Partner Leuchter IT Infrastructure Solutions konnten wir das ambitionierte IT-Security-Projekt zeit- und budgetgerecht umsetzen.»
>
> **RICO ZEMP**
> **Systemadministrator und Security-Verantwortlicher, SGV**

Mit FortiAnalyzer macht Zemp auf ein weiteres wesentliches Leistungsmerkmal aufmerksam. «Dieser ermöglicht ein komfortables Monitoring des gesamten Datenverkehrs zwischen Internet und interner Infrastruktur. So wissen wir jederzeit, was am Perimeter läuft. Zudem sind wir immer aktuell im Bild, wenn eine VPN-Verbindung erstellt oder abgebrochen wird. Funktionen wie Debugging und Auswertung sind ausgesprochen komfortabel und übersichtlich.»

BEREIT FÜR DIE ZUKUNFT

Bei den von der SGV eingesetzten Firewalls handelt es sich um hochleistungsfähige, ASIC-beschleunigte FortiGate-Appliances, die den gesamten Datenverkehr des Unternehmens in Echtzeit filtern und Angriffe abwehren. Damit der Perimeter-Schutz langfristig gewährleistet wird, sorgen Upgrade- und Wartungs-Verträge für stets aktuelle Funktionen, Signaturen und Webfilter-Dienste.

Auch die vorgängig erwähnte Aktivierung weiterer Features spielt hinsichtlich Investitionsschutz und IT-Sicherheit eine zentrale Rolle. Die Funktion «Application Control» beispielsweise erlaubt es, User, Applikationen und Devices auf hoher Ebene zu erkennen und zu kontrollieren. Zudem ermöglicht sie eine granulare Definition, welche Applikationen – oder Teile davon – wann und für wen zugelassen oder gesperrt sind (User based Policy Enforcement).

Ein Ausbauschritt, den die SGV bereits in naher Zukunft angehen wird, ist die Einbindung eines FortiManagers. Diese Hardware-basierte Appliance erlaubt eine zentrale Verwaltung sämtlicher eingebundener UTM-Appliances in Echtzeit. «Wir sind mit moderaten Investitionen in der Lage, unsere IT-Security-Infrastruktur über Jahre aktuell zu halten und unsere Bedürfnisse der kommenden Jahre mit den bestehenden Systemen abzudecken. Dass wir heute von einer derart zukunftsgerichteten Sicherheitsinfrastruktur profitieren, liegt einerseits in der Innovationskraft sowie dem weitsichtigen Produkt-Design des Systemlieferanten Fortinet begründet. Andererseits in der hoch professionellen Zusammenarbeit mit unserem IT-Partner Leuchter IT Infrastructure Solutions. Erfahrung, Know-how und Engagement der kompetenten Crew sind beeindruckend.»

SCHIFFFAHRTSGESELLSCHAFT DES VIERWALDSTÄTTERSEES **(SGV) AG**

Die Schifffahrtsgesellschaft des Vierwaldstättersees (SGV) AG zählt zu den führenden Schifffahrtsunternehmen in der Schweiz. Gemeinsam mit den Tochtergesellschaften Tavolago AG und Shiptec gilt sie als innovatives Kompetenzzentrum für Schifffahrt, Schiffstechnik und Gastronomie. Das kerngesunde Unternehmen erwirtschaftet einen jährlichen Umsatz von rund 60 Mio. Franken, zählt rund 450 festangestellte Mitarbeitende und beschäftigt während der Hauptsaison (Sommer) jeweils bis zu 600 Mitarbeiterinnen und Mitarbeiter.

LEUCHTER IT INFRASTRUCTURE SOLUTIONS AG

Die Leuchter IT Infrastructure Solutions AG ist Teil der Leuchter IT Solutions Gruppe mit dem Hauptstandort in Luzern. Diese bietet in ihren sieben Unternehmungen und mit den über 80 Mitarbeitenden IT-Lösungen und Management-Dienstleistungen im deutschsprachigen Raum an. Kernkompetenz der Leuchter IT Infrastructure Solutions bildet das Planen, Bauen und Betreiben von modernen IT-Infrastrukturen – sowohl vor Ort als auch in der Cloud.

VIERWALDSTÄTTERSEE

Leuchter IT SOLUTIONS

BOLL IT Security Distribution

STARKE PARTNER

KUNDE	REALISATION	DISTRIBUTION
SGV AG	**Leuchter IT Infrastructure Solutions AG**	**Boll Engineering AG**
6002 Luzern	**6003 Luzern** / www.leuchterag.ch	**5430 Wettingen**
www.lakelucerne.ch		www.boll.ch