



SICHER VERNETZT

VINCI ENERGIES SCHWEIZ SETZT AUF FORTINET SECURITY-APPLIANCES

VINCI Energies Schweiz AG optimiert ihr schweizweites Kommunikationsnetz und setzt dabei auf FortiGate-Security-Appliances von Fortinet. Damit schafft das Unternehmen ein Maximum an Sicherheit und Verfügbarkeit.



FORTINET®

Wer mit seinem PW in den Süden fährt, kommt mit grosser Wahrscheinlichkeit mit Systemen und Lösungen des weltweit tätigen VINCI-Konzerns in Berührung. Dann etwa, wenn es darum geht, an Maut-Zahlstellen den Obolus für die Autobahnnutzung zu entrichten. Oder bei der Kommunikation via Handy. VINCI, Arbeitgeberin von rund 180 000 Mitarbeitenden, ist ein stark diversifizierter, multinationaler Konzern. Ein wesentliches Standbein bildet der Konzernbereich VINCI Energies, der einen jährlichen Umsatz von rund 9 Mia. Euro verantwortet und ca. 64 000 Mitarbeitende beschäftigt. Zu den Tätigkeitsbereichen von VINCI Energies, zu der auch die VINCI Energies Schweiz AG gehört, zählen unter anderem die Planung, der Bau und die Pflege von Energie-, Transport- und Kommunikationsinfrastrukturen, Consulting und Engineering sowie die Realisierung und der Betrieb von Gebäudesystemen. Mit ihren Geschäftsstellen an über 50 Standorten – diese firmieren mehrheitlich unter der Bezeichnung ETAVIS – ist VINCI Energies Schweiz in allen Landesteilen präsent.



ENGPÄSSE ERKENNEN – UND VERHINDERN

Die im Laufe der Jahre kontinuierlich gewachsene VINCI Energies Schweiz sah sich in jüngerer Zeit mit Engpässen im Bereich der Daten- und Sprachkommunikation konfrontiert. Die bestehende IT- und Kommunikationsinfrastruktur vermochte den wachsenden Anforderungen hinsichtlich Dienstqualität, Verfügbarkeit, Geschwindigkeit und Sicherheit nicht mehr zu genügen. Dazu Stefan Bürgi, Leiter IT bei VINCI Energies Schweiz: «Eines der Kernprobleme war die Vernetzung der einzelnen Standorte über lediglich ein MPLS WAN. Ein Ausfall dieses nicht redundant geführten Pfades hätte zur Folge gehabt, dass den Standorten wesentliche Anwendungen nicht mehr zur Verfügung gestanden hätten.» Nicht weniger kritisch waren die fehlenden Zugriffsbeschränkungen unter den einzelnen Business-Units. Die eingesetzte «Fully-Meshed» WAN-Technologie verunmöglichte, Zugriffe von einem Standort zum andern zu kontrollieren oder zu verhindern, was nicht zu unterschätzende Sicherheitsrisiken zur Folge hatte. «Die ungehinderte Ausbreitung von Schadcode etwa oder die Gefährdung der Sicherheit durch Fehlkonfigurationen in einzelnen Standorten», so Bürgi. Ferner betont er, dass es in der Vergangenheit nicht möglich war, einzelne Anwendungen zu priorisieren bzw. QoS (Quality of Service) zu garantieren: «Die Ausführung einer Core-Anwendung beispielsweise konnte durch eine erhöhte Internetauslastung negativ tangiert werden.»

Da in den einzelnen Standorten keine Firewalls installiert waren und der gesamte Internet-Verkehr inkl. Web-Filtering über die zentrale UTM-Appliance im Datacenter geführt wurde, war das WAN mit einem zu hohen Datenaufkommen konfrontiert. Dies führte in zunehmendem Mass zu punktueller Netzüberlastung. Ein weiterer Aspekt, welcher die Planung und Umsetzung einer neuen, zukunftsgerichteten Netzinfrastruktur notwendig machte, war laut Bürgi die ausgesprochen heterogene Systemlandschaft. «Diese ergab sich durch die Übernahme diverser Firmen sowie aufgrund der gewährten Standortautonomie. Die heterogene Umgebung verunmöglichte nicht nur ein zentrales Management der Systeme, sondern erschwerte auch die Nutzung moderner Dienste wie etwa Multimediaanwendungen oder die sichere Einbindung mobiler Devices.»

«Die Wahl unseres Planungs- und Umsetzungspartners AXIANS GNS sowie die Entscheidung zugunsten der IT-Security-Lösungen von Fortinet waren goldrichtig.»

STEFAN BÜRGI

IT-Leiter, VINCI Energies Schweiz

ANSPRUCHSVOLLES PFLICHTENHEFT

Angesichts der unbefriedigenden Situation beauftragte VINCI Energies Schweiz die in Winterthur domizilierte AXIANS GNS AG mit der Erarbeitung, Planung und Umsetzung eines neuen Netzwerkkonzepts. Dieses sollte sich durch eine maximale Benutzerfreundlichkeit und -zufriedenheit auszeichnen, hinsichtlich Verfügbarkeit, Performance und Sicherheit Bestmarken setzen und die Einbindung von Multimediaanwendungen sowie von mobilen Devices ermöglichen. Zudem sollte das neue Kommunikationsnetz eine einfache und jederzeitige Einbindung von temporären Standorten und Arbeitsplätzen – z. B. Container bzw. mobile Büros auf Baustellen – ermöglichen. Ein wichtiger Punkt im Pflichtenheft war zudem das zentrale Management und Monitoring der einzelnen Geschäftsstellen und Systeme. Die Umsetzung dieser und weiterer Vorgaben ist dem AXIANS GNS Team auf elegante und effektive Art gelungen. Dies nicht zuletzt dank der firmenweiten Verwendung von Fortinet-UTM-Appliances der FortiGate-Familie. Die ASIC-basierenden, hoch performanten Systeme beinhalten nicht nur klassische Firewallfunktionen zur Sicherung des Netzwerkgateways, sondern zeichnen sich durch die Unterstützung zahlreicher weiterer Features aus. So ermöglichen sie beispielsweise den Aufbau geschützter VPN-Verbindungen, die gezielte Priorisierung einzelner Dienste und folglich den Betrieb von Anwendungen, die auf QoS angewiesen sind – beispielsweise Video- und Sprachdienste. Ebenso bedeutsam ist die in jeder UTM-Appliance integrierte AP-Controller-Funktion. Dieses Leistungsmerkmal ermöglicht die direkte Einbindung von Access Points (FortiAPs)



FORTINET – FÜR EINE UMFASSENDE IT-SECURITY

VINCI Energies Schweiz setzt auf folgende Systeme von Fortinet:

Datacenter

- UTM-Appliance FortiGate 621B Cluster
- FortiAnalyzer
- FortiManager

Mittlere und grosse Standorte

- UTM-Appliance FortiGate 100D (Einzellösung oder Cluster)
- Access Point FortiAP 221B

Kleine Standorte

- FortiWifi 60D – kombinierte UTM-Appliance mit integriertem Access Point



und folglich den Aufbau hoch sicherer WLAN-Infrastrukturen. Sämtliche via WLAN übertragenen Daten werden von der UTM-Appliance auf Schadcode überprüft, was Funknetzen denselben Sicherheitsstandard garantiert, wie dies bei kabelgebundenen Netzen (LAN, WAN) üblich ist.

Ein entscheidender Faktor für die Wahl der UTM-Appliances von Fortinet war zudem die Funktion «Dynamic Routing». Diese kommt an Standorten zum Tragen, die über mehrere Netzverbindungen verfügen. So ist es beispielsweise möglich, mittels Routing-Tabellen beziehungsweise Inbound- und Outband-Rules zu definieren, welche Verbindungen wann genutzt werden sollen. Zu den möglichen Routing-Kriterien gehören u. a. die Kosten pro Pfad, die Gewichtung der jeweiligen Applikation, die aktuelle Belastung der einzelnen Verbindungen oder deren Verfügbarkeit.

STANDORTGERECHTE VERNETZUNG MIT MAXIMALER SICHERHEIT

Um den unterschiedlichen Bedürfnissen der einzelnen Standorte gerecht zu werden – diese reichen von Kleinstniederlassungen mit wenigen Mitarbeitenden über mittelgrosse Standorte bis hin zu grossen Geschäftsstellen mit 25 bis über 100 Mitarbeitenden – hat das Projektteam der AXIANS GNS gemeinsam mit dem Kunden drei Standorttypen mit unterschiedlicher Vernetzung definiert. Markus Hilty, Leiter IT Engineering AXIANS GNS, erklärt: «Alle Standorte sind mit einer FortiGate UTM-Appliance ausgestattet. Diese gewährt vor Ort eine maximale Gateway-Security und ermöglicht eine VPN-basierte, geschützte Kommunikation mit und zu den anderen Standorten sowie zum zentralen Datacenter. Dank der integrierten AP-Controller-Funktion lassen sich zudem sämtliche Standorte mit einem WLAN ausrüsten. Ergänzend dazu sind mittelgrosse Geschäftsstellen mittels MPLS vernetzt und die grössten Niederlassungen sind via Glasfaser direkt mit dem Datacenter verbunden

«Dank Fortinet konnten wir dem anspruchsvollen Pflichtenheft in allen Belangen entsprechen. Aspekte wie Gateway-Security, WLAN-Einbindung, zentrales Management, BGP und QoS sind perfekt realisiert.»

MARKUS HILTY

Leiter IT Engineering, AXIANS GNS

«Direct Links». Dank dieser redundanten, über unterschiedliche Carrier etablierten Vernetzung profitiert VINCI Energies von einer maximalen Verfügbarkeit ihrer Netzinfrastruktur.»

In der von AXIANS GNS geplanten und umgesetzten Architektur können die UTM-Appliances von Fortinet ihre Stärken vollumfänglich ausspielen. So etwa in Form des dynamischen Routings (BGP), das die logischen Verbindungen zwischen dem Datacenter und den einzelnen Standorten regelt, die unterschiedlichen Anschlusstypen (VPN, WAN, Direct Links) berücksichtigt und auch Failover- und Failbackvorgänge definiert. Ebenso wertvoll ist das integrale Bandbreitenmanagement, das die Priorisierung einzelner Applikationen auf der LAN-, WAN- und WiFi-Strecke ermöglicht und somit die benötigte Dienstqualität (QoS) über den gesamten Übertragungsweg garantiert. Nebst der Zuweisung garantierter Bandbreiten lassen sich diese auch limitieren – so etwa auf Ebene Subnetze, Sessions und Protokolle.

Auch hinsichtlich der für alle Standorte vorgesehenen WLAN-Installationen überzeugen die FortiGate-Appliances sowie die Access Points von Fortinet auf der ganzen Linie. Sie ermöglichen die Bildung und Trennung unterschiedlicher virtueller Netze. Folglich lassen sich mittels derselben physischen APs und des zentralen AP-Controllers mehrere unterschiedliche Wireless-Netzwerke mit unterschiedlichen Security-Policies betreiben – so etwa private (interne) und Public-WLANs.

ZENTRALES MONITORING UND MANAGEMENT

Um die verteilte Netz- und Securityinfrastruktur effizient und zentral zu verwalten, hat AXIANS GNS das Datacenter von VINCI Energies Schweiz mit einem FortiManager bestückt. Dabei handelt es sich um eine eigenständige Appliance, die eine zentrale Konfiguration und Überwachung der angemeldeten FortiGate-Appliances erlaubt – unabhängig davon, an welchem Standort sich diese befinden. Auch das Einspielen neuer Signaturen lässt sich zentral verwalten. Ergänzend dazu erlaubt eine mit FortiAnalyzer bezeichnete Appliance ein zentrales Logging und Reporting sämtlicher dezentral eingesetzter FortiGate-Firewalls sowie eine zentrale Analyse der Netzwerkaktivität, des Webverkehrs und der erfolgten Attacken. Die von den einzelnen Appliances erstellten Log-Records werden über verschlüsselte VPN-Tunnels an den FortiAnalyzer übermittelt. Dazu Markus Hilty: «Sicherheit auf der ganzen Linie. Mit Fortinet setzen wir auf ein hoch innovatives Unternehmen im Bereich der IT-Security. Davon profitieren unsere Kunden und wir gleichermassen.»



AXIANS GNS AG

Die AXIANS GNS, eine Tochtergesellschaft der VINCI Energies Schweiz, wurde 1995 gegründet, beschäftigt rund 30 Mitarbeitende und erwirtschaftet einen jährlichen Umsatz von mehr als 13 Mio. Franken. Zu den unter der Dachmarke AXIANS angebotenen Dienstleistungen zählen konvergente und skalierbare IT-Infrastrukturlösungen zur sicheren Sprach-, Daten- und Videokommunikation. Eine wichtige Komponente bildet dabei der Bereich IT-Security, der führende Lösungen für Themen wie Firewalling, Content Security, Web Application Security, Authentication, Autorisation und E-Mail Encryption beinhaltet.



VINCI Energies Schweiz AG

VINCI Energies Schweiz, Teil der weltweit operierenden VINCI Energies, hat sich schweizweit als Partner für integrale Gebäudetechnik sowie für Telekominfrastrukturen etabliert. Das Unternehmen, das beinahe 2100 Mitarbeitende beschäftigt und rund 350 Lernende ausbildet,

erwirtschaftet mit seinen mehr als 50 Niederlassungen einen jährlichen Umsatz von nahezu 390 Mio. Franken. VINCI Energies Schweiz konzentriert sich auf die Planung, Projektleitung, Realisierung und den Betrieb von Systemen in der Elektrotechnik, Telematik und ICT (In-

formations- und Kommunikationstechnologie). Schwerpunkte bilden Themen wie Automationstechnik, Schaltanlagenbau, technisches Gebäudemanagement, industrielle Instandhaltung und Energieoptimierung.



STARKE PARTNER

KUNDE

VINCI Energies Schweiz AG
8021 Zürich
www.vincienergiesschweiz.ch

REALISATION

AXIANS GNS AG
8404 Winterthur
www.axians.ch

DISTRIBUTION

Boll Engineering AG
5430 Wettingen
www.boll.ch
