Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

SECUREPOINT

IT-Sicherheitslösungen für die Schifffahrt

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Securepoint Case Study

IT-Sicherheitslösungen für die Schifffahrt

Vernetzt auf hoher See

Die Mitglieder von Schiffsbesatzungen sind enormen Belastungen ausgesetzt und von von Familie und Freunden oft monatelang isoliert. Mit Smartphone oder Notebook können sie über das Schiffsnetzwerk per Satellit im Internet surfen sowie persönliche Kontakte pflegen. Doch diese Geräte sind ein beliebtes Einfallstor für Cyber-Angriffe.

Denn: Dank moderner Satellitenverbindung bleiben moderne Handelsschiffe meist durchgehend mit dem Festland verbunden. Über die an Bord installierte IT-Infrastruktur werden sensible und wichtige Daten für den operative Schiffsbetrieb mit der Reederei permanent ausgetauscht. Auf modernen Schiffen werden immer mehr Komponenten über Schiffsnetzwerke und Software gesteuert. Dadurch wird ihre IT-Infrastruktur verwundbar. Mit steigender Vernetzung erhöht sich das Risiko für Cyber-Angriffe.

Digitale Sicherheit als Herausforderung

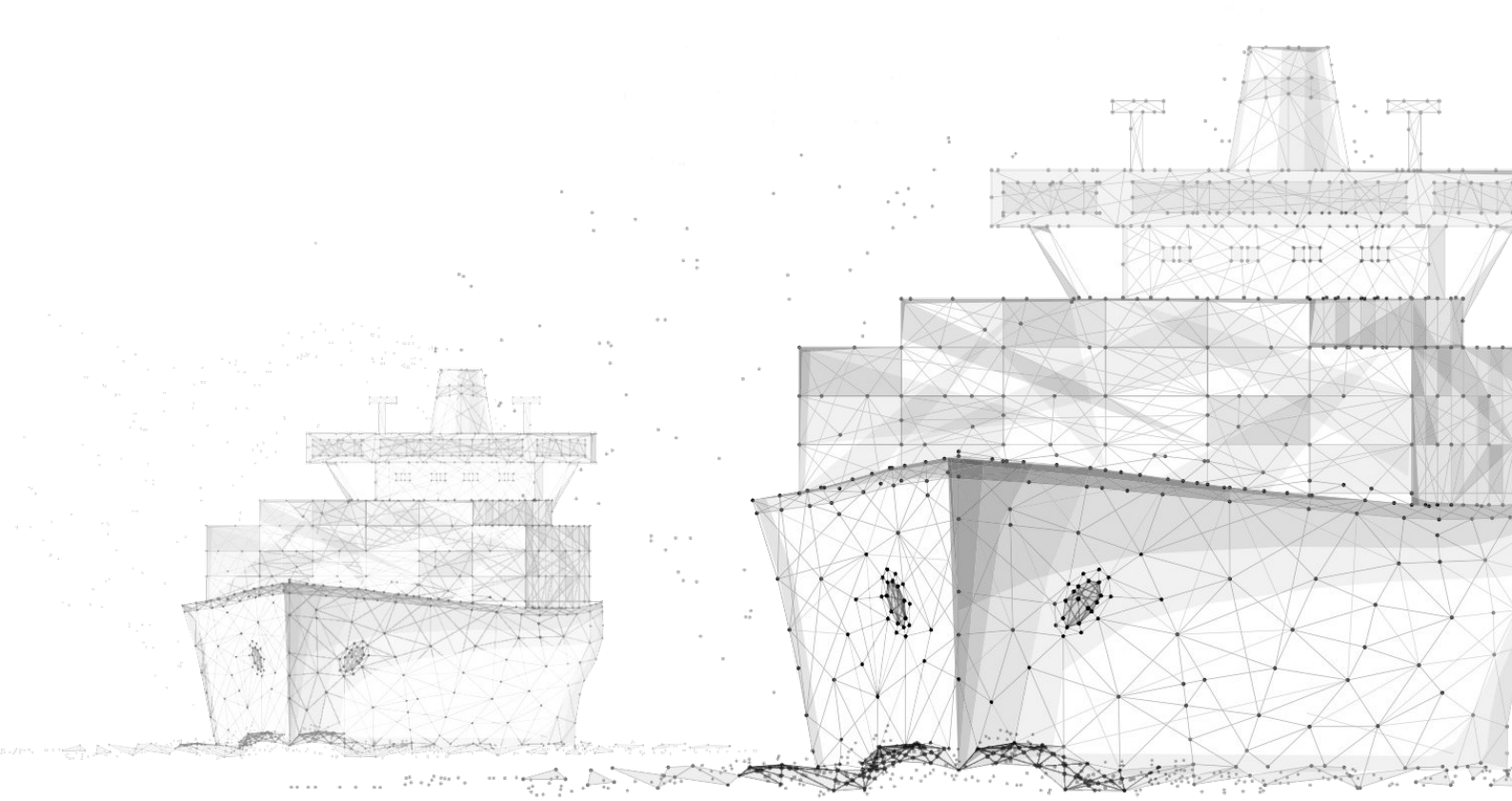
Die Digitalisierung der Schifffahrt ist in vollem Gange. Für die maritime Branche ergeben sich dadurch neue Wertschöpfungsketten und Möglichkeiten zur Effizienzsteigerung. Ein Grund dafür ist die Bedeutung der Branche: Heute werden 95% des interkontinentalen Warenaustausches durch die Schifffahrt geleistet. Laut des Bundesministeriums für Wirtschaft und Energie setzt die Branche allein in Deutschland ca. 50 Milliarden Euro jährlich um. Um dem gerecht zu werden, haben die deutsche Bundesregierung und die maritime Wirtschaft in der Maritimen Agenda 2025 die Digitalisierung als zentrales Handlungsfeld benannt.

„Mit zunehmendem Datenaustausch zwischen Schiffen, Reedereien, Hafenbetrieben, Offshore-Anlagen, Behörden und weiteren Kommunikationspartnern an Land steigt für alle Beteiligten das Risiko von Cyber-Angriffen. Für alle Akteure in der maritimen Wirtschaft ist es wichtig, dass die involvierten IT-Systeme möglichst umfassend vor Cyber-Angriffen geschützt werden“ (Gemeinsame Erklärung zur Digitalisierung in der maritimen Wirtschaft, Bundesregierung und die maritime Wirtschaft, Hamburg, 4. April 2017)

Wie im IT-Sicherheitsgesetz definiert, gehören Schifffahrtsunternehmen zu den kritischen Infrastrukturen.

Betreiber sind zur Umsetzung von IT-Sicherheitsmaßnahmen verpflichtet.

In diesem Zusammenhang erklärte das Maritime Safety Committee im Juni 2017 das Cyber Risk Management zum Teil des ISM-Codes. Maßnahmen zur Organisation eines sicheren Schiffsbetriebs und zum Schutz der Menschen an Bord gehören damit zur Pflicht für die internationale Schifffahrt. Die Umsetzung muss bis zum Jahr 2021 erfolgen.



Cyber-Piraten auf Kaperfahrt

Welche Bedeutung die IT-Sicherheit auf Schiffen und der Schutz der Crew hat, wurde spätestens mit der #NotPetya-Attacke Ende Juni 2017 deutlich. Computer wurden mit Schadsoftware infiziert, die Angreifer verschlüsselten Daten und verlangten Lösegeld. #NotPetya befiel knapp 80 Häfen weltweit. Große Flotten von Containerschiffen waren tagelang außer Gefecht gesetzt. Unter den Opfern der digitalen Erpressung waren mehrere europäische Reedereien, darunter eine der größten Containerschiffsreedereien der Welt. Auch Angriffe auf das elektronisches Navigationsinformationssystem Electronic Chart Display and Information System (ECDIS) gab es bereits.

Laut des Global Risk Reports 2019 des 14. Weltwirtschaftsforums sind auch in Zukunft große wirtschaftlichen Schäden durch umfangreiche Cyber-Attacken oder Malware sowie massive Vorfälle von Datenbetrug und Datendiebstahl zu erwarten.

Ausgangssituation

Die Information Technology Engineering (ITE) GmbH seht für moderne IT-Infrastruktur für Reedereien und Seeschiffe. Das Hamburger Unternehmen bietet mit „ITE connect“ Kunden innovative Sicherheitslösungen für die Schifffahrt und die maritime Wirtschaft.

ITE supported weltweit auf rund 250 Schiffen die IT-Infrastruktur. Zu Ihren Kunden gehören unter anderem namhafte Reedereien aus Hamburg und Bremen sowie international ausgerichtet Reedereien aus Asien.

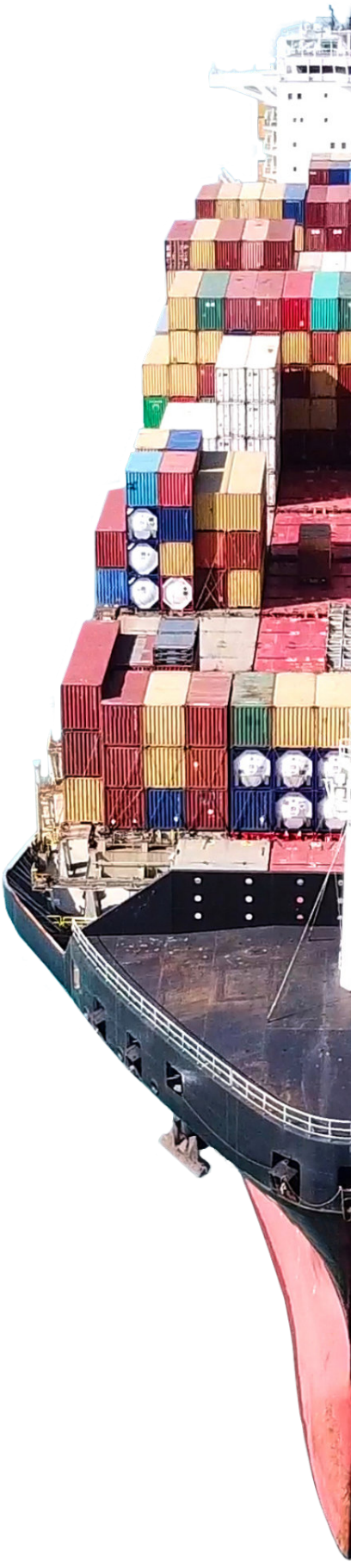
Seit Anfang 2018 setzt das Unternehmen die NextGen UTM-Firewalls des deutschen Herstellers Securepoint ein. Aus diesem Zusammenspiel entstand die Sicherheitslösung ITE connect: Die Crew kann sicher surfen und das Schiffsnetzwerk wird umfangreich geschützt.

„Unser Projektziel war es einerseits einen sicheren, kontrollierten Internetzugang für die Crew-Mitglieder einzurichten und zum anderen das Schiffsnetz von Land aus über einen VPN-Gateway zu konfigurieren sowie zu warten“, erläutert Frank Eggert, Geschäftsführer der ITE.

Bei Hamburger und Bremer Reedereien sorgt ITE connect inkl. Securepoint NextGen UTM-Firewalls bisher 62 Mal für Sicherheit:

„Überzeugt hat uns bei den Lösungen von Securepoint die schnelle Einrichtung des VPN-Gateways zwischen Schiffen und Festland. Das liegt sicher mit daran, dass das Firewall-Image nur 70MB groß ist. Wichtig war uns auch, dass die eingesetzte Lösung die Vorgaben der europäischen Datenschutz-Grundverordnung einhält. Securepoint erfüllt da alle Erwartungen und setzt garantiert keine Hintertüren ein. Das ist für uns ein klares Statement. Der professionelle Support des Herstellers war dann das i-Tüpfelchen,“ sagt Frank Eggert.

Auch die hohe Qualität des High-End Content-Filters inkl. Zero-Hour-Protection sowie das integrierte Einmalpasswortsystem haben den Ausschlag gegeben, die Securepoint NextGen UTM-Firewall einzusetzen.



Mit Sicherheit über die Weltmeere

Über das Internet verbreiten sich digitale Bedrohungen durch Schadsoftware oder Malware rasend schnell. Die Zeit zwischen dem Auftreten neuer Gefahren und ihres Eintreffens bei einzelnen Benutzern in der Reederei oder auf dem Schiff wird immer kleiner. Klassische Verfahren bieten dafür oft keine Lösungen.

„ITE connect“ ist die Antwort auf diese Herausforderung. Integriert in „ITE connect“ bildet die Securepoint NextGen UTM-Firewall von Securepoint den Rumpf zum Schutz Ihrer maritimen Flotte und Ihrer IT. Mit all ihren Features ist „ITE connect“ die Sicherheitslösung für die maritime Wirtschaft. Sie verschafft Reedereien und Schiffen sichere Internetnutzung, ein sicheres Netzwerk, sichere Konnektivität und sichere Kommunikation via E-Mail. Dabei hilft eine zentrale Technologie der Securepoint NextGen UTM-Firewall: die Cyber Defence Cloud. Durch Machine Learning, Schwarmintelligenz, Data-Mining, leistungsstarke Protokolle und das Know-how das Analyseteams werden Erkenntnisse aus technischen Innovationen sowie von Menschen miteinander verknüpft.

Profitieren Sie von der Mehrwertdienstlösung, die in Kombination mit professionellen IT- und Kommunikationssystemen wie 3g / 4g (und zukünftig 5g), FBB oder VSAT verwendet werden kann, ohne an einen bestimmten Provider gebunden zu sein. "ITE connect" kann jederzeit an Bord Ihrer maritimen Flotte installiert oder nachgerüstet werden. „ITE connect“ ist ebenfalls als vollständig integrierter Bestandteil der umfassenden ITE-Schifffahrt verfügbar.

„ITE connect“ bietet Homogenität und zentrale Verwaltung Ihrer Flotte für Web- / Mail-, Internet- und Cyber-Sicherheit.

"ITE connect" bedeutet "ready to use" und arbeitet unabhängig von Sendezeit-anbietern.

„ITE connect“ bedeutet:

Sicheres Surfen

Der High-End Content-Filter ist als wichtiges Sicherheitsfeature Teil der Cyber Defence Cloud. Er überzeugt auf der in „ITE connect“ integrierten NextGen UTM-Firewall mit hoher Genauigkeit, Schnelligkeit und geringem Ressourcenverbrauch. Der Threat Intelligent Feed ist die wichtigste Kategorie der Cyber Defence Cloud. Die über das Schiffsnetz aufgerufenen IPs und URLs werden auf Spare-/Phishing, Ransomware, Malware- bzw. Makro-Download und andere Gefahren geprüft. Verbotene, gefährliche oder anstößige Inhalte werden so blockiert. Reedereien erfüllen damit ihre Sorgfaltspflicht und setzen die gewünschten Zugriffsbeschränkungen sowie interne Sicherheitsregeln durch. Damit sind sie auch vor möglichen Haftungsansprüchen geschützt, die durch Fehlverhalten von Angestellten bei Nutzung firmeneigener Geräte geltend gemacht werden können.

Sichere E-Mails

Mail-Security auf einem neuen Level: mit Quarantäne gefährlicher E-Mails direkt auf der integrierten NextGen UTM-Firewall und einem selbstentwickelten Zeitschloss für verdächtige Nachrichten. Nach definierter Zeit werden die E-Mails erneut geprüft und erst zugestellt, wenn kein Sicherheitsrisiko besteht. Das Ergebnis: 99,9% weniger Spam/Viren und eine maximal reduzierte Fehlerquote bei der Erkennung. Das Scannen von 25 Milliarden E-Mails in der Cyber Defence Cloud pro Tag macht das möglich. Für Schiffsnetzwerke und Reedereien bedeutet das einen höchstes Maß an Sicherheit. Daten können durch Sorglosigkeit oder Unwissenheit der Nutzer so kaum noch in die falschen Hände geraten. Die Gefahr der Kompromittierung des ganzen Netzwerkes wird damit minimiert.

Sichere Verbindungen

Durch VPN-fähige UTM-Gateways lassen sich beliebig viele Standorte sicher vernetzen, egal ob PC-Arbeitsplätze in der Reederei oder Superintendent-Laptop innerhalb des Schiffsnetzwerks. Der Securepoint SSL-VPN Client ermöglicht mobilen Mitarbeitern einen verschlüsselten VPN-Zugang zum Unternehmensnetzwerk inkl. sicherem Internetnutzung. Dem einzelnen Benutzer lassen sich dynamisch anpassbare Regelwerke zuweisen.

Mailserver-Administrationsübersicht

Das Ziel einer einfachen und gleichzeitig leistungsfähigen Schnittstelle für alle Systemverwaltungsaufgaben wird bei „ITE connect“ mit dem Mail Admin erfüllt. Mit diesem webbasierten Tool werden die integrierten E-Mail-Konten sowie die gesamte Konfiguration des Mail-Servers und seiner Komponenten verwaltet. Die Fähigkeit, ein nativ implementierter Bestandteil in einer Microsoft Active Directory-Umgebung zu sein, macht eszu einer perfekten Ergänzung innerhalb des Netzwerks Ihres Schiffes.

Virtuelle Domäne

Es können beliebig viele virtuelle Domänen erstellt werden. Dafür muss nur der Domainname für E-Mail-Konten der jeweiligen Benutzer angegeben werden. Zudem können Aliase für eine virtuelle Domäne festzulegt werden, sodass das Senden einer E-Mail an eine virtuelle Domäne oder an einen ihrer Aliase transparent wird.

E-Mail-Filter

Der E-Mail-Server kann so konfiguriert werden, dass er einen Inhaltsfilter für Nachrichten verwendet. Dazu muss der Filterserver die Nachricht von einem bestimmten Port empfangen und das Ergebnis an einen anderen Port zurücksenden, an dem der Mailserver die Antwort abhören muss. Sie können einen benutzerdefinierten E-Mail-Filter auswählen oder den integrierten E-Mail-Filter verwenden, der standardmäßig verwendet wird.

Protokolle

Es werden Standardprotokolle wie POP3 (S), IMAP (S) oder SMTP sowie CardDAV, CalDAV und SIEVE unterstützt.

Protokollierung

Mail Admin stellt eine Infrastruktur bereit, die es den Modulen ermöglicht, alle Arten von Ereignissen zu protokollieren, die für den Administrator möglicherweise nützlich sind. Diese Protokolle sind über die Webschnittstelle verfügbar. Protokolle werden in einer Datenbank (MySQL®) gespeichert, sodass Abfragen, Berichte und Aktualisierungen einfacher und effizienter sind.

Webmail-Lösung

Teilen Sie Ihre E-Mails, Kalender und Adressbücher in Ihrem Unternehmensnetzwerk mit unserer Webmail-Lösung. Es bietet eine umfassende AJAX-basierte Webschnittstelle und unterstützt mehrere native Clients mit Standardprotokollen wie CalDAV, CardDAV und GroupDAV sowie Microsoft ActiveSync. Die Komponente kommt nicht als einfacher Webmail-Client daher, sondern funktioniert als Groupware-Lösung. Diese befindet sich mitten auf den Servern und bietet Ihren Benutzern eine einheitliche und vollständige Schnittstelle für den Zugriff auf ihre Informationen. Als Einsatzorte bieten sich kleine Unternehmensumgebungen mit nur wenigen Mitarbeitern sowie Produktionsumgebungen an, an denen Tausende von Benutzern beteiligt sind.

Securepoint GmbH
Bleckeder Landstraße 28, 21337 Lüneburg
Tel.: 0 41 31 / 24 01-0
www.securepoint.de | info@securepoint.de

Crew-Internet und Dashboard

Das Internet wird durch ein auf W-LAN basierendes Internet der Crew an Bord von Schiffen bereitgestellt und verfügt über einstellbare Datenübertragung sowie Zeit- und Bandbreitenbeschränkungen. Hunderte von Geräten wie Smartphone, Laptop, Tablet und viele mehr sind leicht zugänglich. Über das zentrale Management-Dashboard können Sie Netzwerke, Geräte und einzelne Benutzer überwachen und Ereignisse jederzeit und von jedem Ort aus melden und verwalten.

Profile

„ITE connect“ arbeitet mit dem Prinzip der Benutzerprofile. Es können alle denkbaren Varianten aus Volumen und Zeit als Profile für die einzelnen Nutzer hinterlegt werden, um alle Anforderungen an Bord zu erfüllen.

Erstellung von Vouchern

Voucher sind die traditionelle Art und Weise, wie Wifi Hotspot-Benutzer ihre Zugangsdaten erhalten. Sie werden immer noch in vielen Situationen verwendet und ITE Internet macht die Erstellung und Verteilung von Gutscheinen schnell und einfach. Gutscheine erhalten ein Profil, um den Benutzer nach Bedarf einzuschränken. Die Gutscheine können dann im PDF-Format erstellt werden, um vom System aus per E-Mail gesendet oder gedruckt zu werden. Gutscheine können zeitlich begrenzt sein.

Permanente Benutzer

Wenn Sie das Thema der Benutzerflexibilität fortsetzen, muss möglicherweise ein Benutzer dauerhaft auf ein WLAN-Netzwerk zugreifen. Ein Seemann kann beispielsweise für 3 Monate angemeldet sein und muss auch ohne Voucher auf das Internet zugreifen können. Nachdem der Seemann als permanenter Benutzer zum System hinzugefügt wurde und seine erste Anmeldung vorgenommen hat, kann er für den vordefinierten Zeitraum mit den vordefinierten Profilen, die von der ITE-Internetlösung überwacht und gesteuert werden, auf das Internet zugreifen.

Captive-Portal mit dynamischen Anmeldeseiten

Ein Captive-Portal kann als Access Control-Komponente eines WLAN-Netzwerks bezeichnet werden. Das Captive-Portal kommuniziert mit dem Server, um den Zugriff auf das Internet zu erlauben oder zu verweigern.

Über Securepoint

Securepoint Unified Security bedeutet: Sicherheit vom ersten Gedanken bis zum letzten Bit. Die ganzheitliche Sicherheitsstruktur des deutschen Herstellers legt sich wie die Schichten einer Zwiebel schützend um die IT von Partnern und Kunden. Mit NextGen UTM-Firewalls, E-Mail-Archivierung, Antivirus Pro und Mobile Security schützt die Sicherheitsstrategie der Securepoint Unified Security die IT-Infrastruktur kleiner und mittlerer Unternehmen (KMU). Weltweit werden so bereits mehr als 50.000 Netzwerke abgesichert.

Als inhabergeführter Hersteller ist Securepoint im Bereich der NextGen UTM-Firewalls in Deutschland führend. Das Portfolio des Unternehmens wird von einem einfachen Management gesicherter WLAN-Verbindungen (BYOD), einem Management-System für alle Module und unterschiedlichsten Schulungsangeboten komplettiert.

Der Hersteller lässt die Sicherheit der eigenen Betriebssysteme, Software und Dienste ständig überprüfen. Die Sicherheitsstruktur der Securepoint Unified Security wird durch regelmäßige Pentests zusätzlich von unabhängigen Dritten auf Herz und Nieren getestet.

Durch permanente technische Weiterentwicklung der Hard- und Software sowie die qualifizierte Unterstützung durch einen eigenen Herstellersupport erreicht Securepoint eine hohe Kundenzufriedenheit. Alle Produktspezialisten im Support sind ausgebildete Fachinformatiker. So erreicht Securepoint einen der schnellsten und zuverlässigsten Support-Angebote am Markt.

Mit dem TeleTrusT Qualitätszeichen „IT Security made in Germany“ versichert das Unternehmen, dass alle selbstentwickelten Lösungen frei von Backdoors sind.

Seit der Unternehmensgründung im Jahre 1997 nimmt das Wachstum des Herstellers stetig zu; in den letzten Jahren um durchschnittlich 30%. Zurzeit sind am Lüneburger Hauptsitz sowie in den Niederlassungen Potsdam, Velbert/Düsseldorf und Stuttgart insgesamt 140 Mitarbeiterinnen und Mitarbeiter beschäftigt.