[sysob]::: ®
IT-Unternehmensgruppe

Whitepaper

Einblicke in das
IT-Security-Angebot bei sysob

[sysob]::: ®
IT-Unternehmensgruppe

WHITEPAPER

Inhaltsverzeichnis

Einleitung: Sind Sie auch im Club der Verunsicherten?

Kennen Sie auch diese latente Unruhe, das Gefühl, auf der Hut sein zu müssen, alles in den passenden Schutz zu investieren – für das IT-Sicherheitskonzept in Ihrem Unternehmen? Dann sind Sie nicht allein im Club der Verunsicherten. Der allgemeine Medientenor zum Thema IT-Sicherheit bzw. (neudeutsch) Cybersecurity lässt zurzeit nur einen Schluss zu: Es gibt kein Entrinnen vor digitalen Angriffen! Und darüber hinaus haben es nicht nur Cyberkriminelle, sondern auch Regierungsbehörden auf Ihre Daten abgesehen! Zweifelsfrei verschärft sich die Bedrohungslage, wie auch IBM-Experten feststellten: Cyberkriminelle sollen im Jahr 2014 mindestens eine Milliarde digitale Datensätze mit persönlichen Informationen gestohlen haben (Quelle: IBM X-Force Threat Intelligence Quarterly).

Aber kopflose Panik ist hier die falsche Reaktion. 100 %iger Schutz lässt sich ohnehin nicht gewährleisten. Ein überlegtes Konzept mit Lösungen zur Vorbeugung und ebenso für die Reaktion auf Vorfälle ist wesentlich sinnvoller. Mit welchen Produkten aus dem sysob-Portfolio dies realisierbar ist, erklärt dieses Whitepaper.

Qualitätsmerkmal „Made in Germany"

Snowden, NSA, Überwachungsskandal – das sind Schlagworte aus den vergangenen Jahren, die vielen Geschäftsführern und IT-Teams bis heute (und wahrscheinlich noch eine ganze Zeit) in den Ohren nachhallen. Viele Unternehmen haben aus den Enthüllungen ihre Konsequenzen gezogen und ihre IT-Sicherheitsstrategie überdacht. Beispielsweise wurde geprüft, ob die installierten Security-Lösungen nicht vielleicht Backdoor-Zugänge und damit potenzielle Schwachstellen aufweisen, die Dritte wiederum zur Spionage nutzen können.

Doch warum selbst prüfen, wenn es andere bereits getan haben? Nachgewiesene Sicherheit bietet das TeletrusT-Qualitätssiegel „IT Security made in Germany". Es belegt, dass keine Backdoors in die Lösungen eingebaut sind, über die Dritte Zugriff auf Computersysteme erlangen und Daten ausspähen könnten.

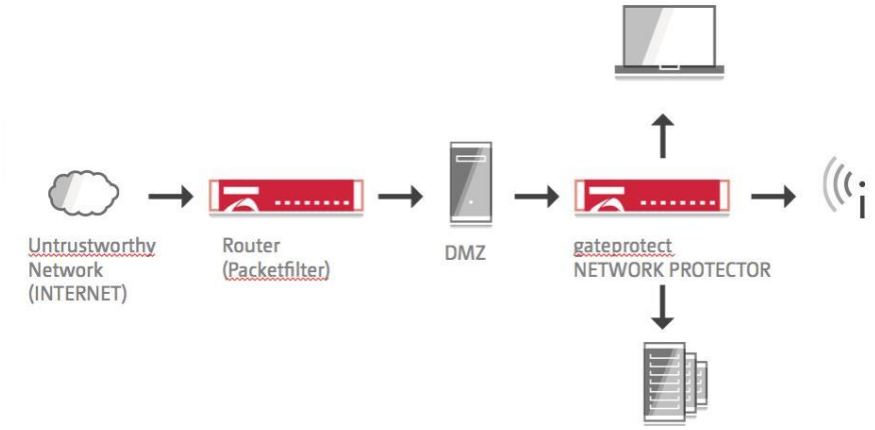
sysob steht voll hinter dem „IT Security made in Germany"-Konzept und hält daher entsprechend deklarierte Sicherheitslösungen bereit, u.a. von Herstellern wie sayTEC und gateprotect. Welche Anforderungen mit diesen Produkten abgedeckt werden können und welche Lösungen sysob für weitere Security-Bereiche
wie Verschlüsselung, Informationsmanagement etc. bereithält, legen die folgenden Kapitel dar.

Das TeleTrusT-Qualitätssiegel „IT Security made in Germany“

Die gateprotect-Methode: Was der Scanner nicht kennt …

Dem Bereich Netzwerksicherheit in Form von Next Generation Firewalls (NGFs) widmet sich die gateprotect GmbH, ein Unternehmen der Rohde & Schwarz-Firmengruppe. Speziell für kleine Betriebe und den Mittelstand werden UTM-Lösungen entwickelt; die NGF Network Protector richtet sich eher an große Unternehmen. Auch Managed Security- und VPN-Client-Systeme zur vernetzten Anbindung von Zweigstellen und Home Offices zählen zum Angebot. Neben dem Qualitätssiegel „IT Security made in Germany“ verfügt gateprotect auch über Nachweise zur Erfüllung höchster internationaler Standards: So zertifizierte das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Firewall-Packet-Filtering-Core der Neuentwicklung im März 2013 nach „Common Criteria Evaluation Assurance Level 4+ (EAL 4+)“. Bei gateprotect zudem selbstverständlich ist persönlicher deutschsprachiger Support.

Die NGF Network Protector arbeitet nach der Prämisse: *„Was der Scanner nicht kennt, akzeptiert er nicht.“* Das bedeutet, die Lösung erlaubt nur eindeutig identifizierten und als vertrauenswürdig bewerteten Elementen den Netzwerkzugang. Jede einzelne Netzwerktransaktion wird auf Anwendungsart und Inhalt analysiert, und nur solche Übertragungen werden durchgelassen, die vollständig verstanden und validiert sind. Diese sogenannte Positivvalidierung verhindert zuverlässig das Eindringen von (unbekannter) Malware. Damit das Risiko von Bedienfehlern möglichst gering ist, achtet gateprotect auf eine möglichst einfache, intuitive Bedienung. Bei den NGFs läuft dies über das Command Center, die zentrale Kontrolloberfläche für das Management komplexer Netzwerkstrukturen. Dank eGUI-Technologie profitieren IT-Verantwortliche von einer herausragenden Übersicht. Sie bietet u.a. sofortiges visuelles Feedback jeder Einstellung sowie eine Layer- und Zoom-Funktion für Netzwerke für bis zu 10.000 User. So wird auch die Firewall-Administration durch eine vollständige visuelle Darstellung des Unternehmensnetzwerkes immens vereinfacht.

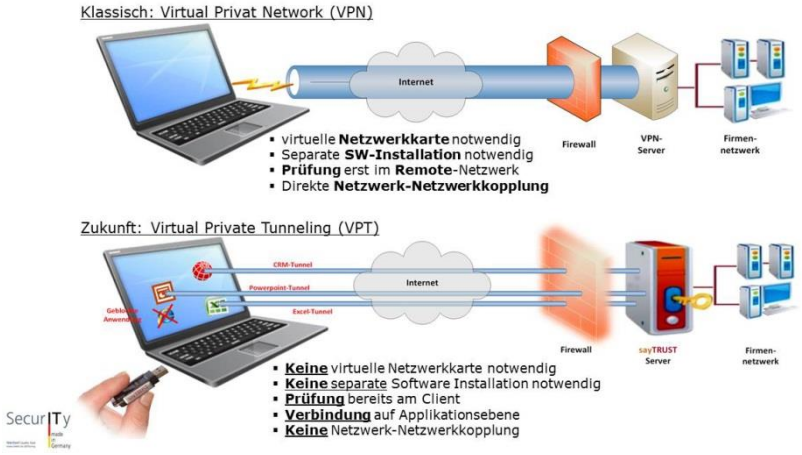


Die Funktionsweise des gateprotect Network Protector

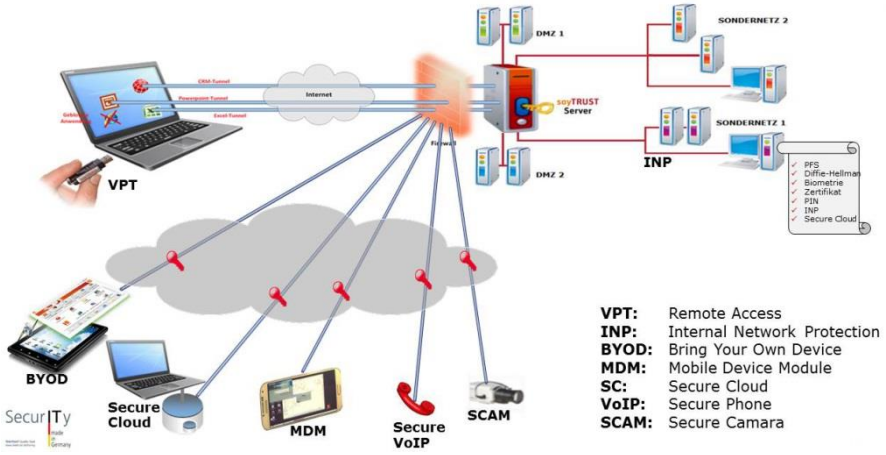
sayTEC entwickelt VPN mit höherer Sicherheit

Das deutsche Unternehmen sayTEC Solutions ist Hersteller von Remote Access-, Backup-, Storage- und Serverlösungen und zudem Entwickler der VPT (Virtual Private Tunneling)-Technologie. Dabei handelt es sich um eine Weiterentwicklung der VPN-Methode. VPT ermöglicht hochsichere Remote-Zugriffe und interne Netzwerksicherheit sowie abhörsichere IP-Telefonie, Secure Cloud, MDM und BYOD. Wie oben erwähnt, ist sayTEC Träger des TeleTrusT-Qualitätssiegels „IT Security made in Germany".

Grundlage der VPT-Technologie ist die Kombination eines Servers und einer Client-Komponente in Form eines USB-Sticks, einer SD-Card oder einer App. Im Gegensatz zur konventionellen VPN-Methode entsteht hier die Verbindung zwischen Server und Client auf Applikationsebene – ohne direkte Netzwerkkopplung. Zusätzlich prüft der sayTRUST Access Server mittels Black- und White-Listen, welche Programme ein Benutzer oder eine Gruppe verwenden darf. Alle nicht freigegebenen Anwendungen werden vom Tunnel ausgeschlossen. Auf diese Weise lassen sich unerwünschte Client-Anwendungen gezielt verbieten.



Übergang von der VPN- zur VPT-Technologie



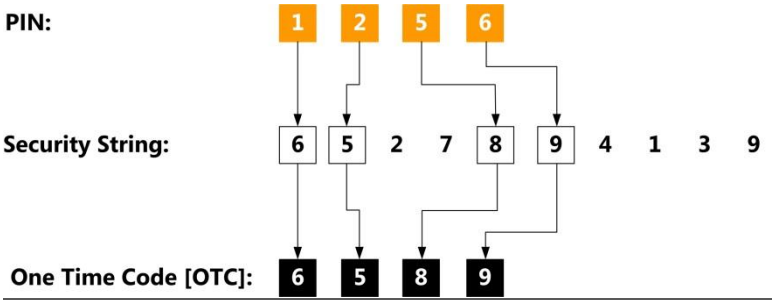
Möglichkeiten mit der VPT-Technologie

Authentifizierung: Bei Swivel reichen vier Ziffern aus

Auf die sichere Erkennung von Nutzeridentitäten hat sich auch Swivel Secure spezialisiert. Die sowohl als Software als auch als Appliance erhältliche, patentierte Multi-Faktor-Authentifizierungslösung ermöglicht individuell anpassbare Kontrollfunktionen für Firmen jeder Größe. Die Lösung wird ergänzt durch PINsafe, der patentierten Extrahierungstechnologie für Einmal-Codes (One Time Code Extraction Protocol (OTC)). Große Blue Chip-Unternehmen als auch KMU und der öffentliche Dienst nutzen die Swivel-Authentifizierungsplattform bereits.

Um seine Identität nachzuweisen, benötigt der User nur eine persönliche PIN, die zur Zufallsgenerierung eines Security-Codes benötigt wird. Je nach Vorliebe des Anwenders wird dieser Code anschließend auf verschiedene Weisen übermittelt: z.B. per SMS, Apps oder als verschleiertes, nicht maschinenlesbares TURing-Bild auf einer VPN Login-Seite. Mithilfe der PIN

bestimmt der Nutzer, welche Zahlen des Security-Codes in welcher Reihenfolge als Einmal-Passwort eingegeben werden müssen. Der One Time Code ist bis auf zehn Stellen erweiterbar, der User selbst muss sich jedoch nur seine PIN (vier- bis zehnstellig möglich, je nach Sicherheitsanforderung) merken.

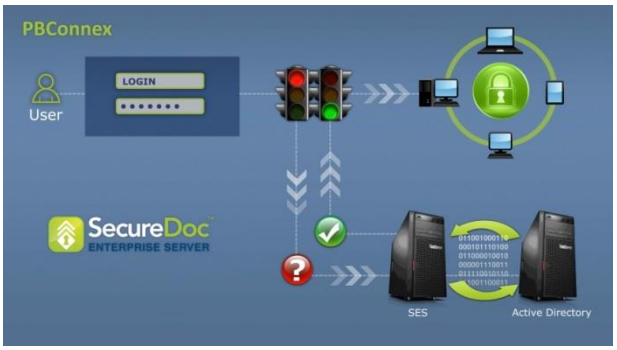


Das Swivel-Protokoll: PIN und Sicherheitszeichenfolge (Security String) generieren einen One Time Code

Sicherheit schon vor dem Booten mit WinMagic

Sichere Verschlüsselungstechnologien sind die Kernkompetenz von WinMagic. Das kanadische Unternehmen ist aufgrund seiner fast 20-jährigen Erfahrung einer der Vorreiter und Innovatoren im Bereich Verschlüsselungs- und Datensicherheitslösungen. Die Zahl an Unternehmen und Regierungsorganisationen weltweit, die auf WinMagic vertrauen, geht in die Tausende. Mit den Lösungen lassen sich Geschäftsrisiken reduzieren, Compliance-Anforderungen erfüllen und sensible Datenbestände vor unerlaubtem Zugriff schützen.

Was WinMagic von anderen Anbietern unterscheidet, ist u.a. die Pre-Boot Networking-Funktion PBConnex. Sie ist eine bislang einzigartige Technologie für die Netzwerkauthentifizierung vor dem Systemstart, die es ermöglicht, verschlüsselte Systeme einfach, kostengünstig und zentral zu verwalten. Alle Daten sind so lange geschützt, bis ein Benutzer sich eindeutig authentifiziert hat. Das WinMagic-Zugpferd ist jedoch die Lösung SecureDoc, die in verschiedenen Ausführungen je nach Unternehmensgröße, Plattform und Anwendungsbedarf (Server, Mac, Windows, Linux, USB-Sticks, Cloud etc.) erhältlich ist. Vertrauliche Daten werden sicher verschlüsselt, und die Authentifizierung unterstützt verschiedene Methoden; darunter Passwortvergabe, Hardware-Token, Biometrie oder Public Key Infrastructure-Lösungen (PKI).



PBConnex von WinMagic

ARTEC managt Big Data

Zu einem professionellen Security-Konzept zählt mittlerweile auch das digitale Informationsmanagement – insbesondere seit durch das Aufkommen von Big Data riesige Datenmengen gehandhabt werden müssen. Darauf konzentriert sich die ARTEC IT Solutions AG. Ihre Lösungen ermöglichen sichere und rechtskonforme Recherche, Wiederherstellung und Aufbewahrung von E-Mails, gedruckten Dokumenten, Dateien oder Sprach- und Telefondaten. Die Kernprodukte sind das Informationsmanagementsystem VSTOR, die Massenspeicherproduktreihe VSTOR Vault sowie die Archivierungslösung EMA (Enterprise Managed Archive).

ARTEC wertet die Produkte EMA und VSTOR zusätzlich durch die Konzepte „Trusted EMA" und „Trusted VSTOR". Dadurch entstand die weltweit erste Appliance für Archivierung, Informationsmanagement und Big Data, die nach dem Trusted Computing Standard (TC) aufgebaut ist und durch ARTEC-eigene Entwicklungen angepasst wurde. Trusted EMA/Trusted VSTOR basieren auf einem Trusted Platform Module (TPM)-Chip, der in den Appliances fest verankert ist. Dadurch verschmelzen Hardware und Appliance-Software zu einer untrennbaren Einheit. Der gerätebezogene Schlüssel zu den archivierten/gespeicherten Daten wird durch den TPM-Chip und das Trusted Computing-Konzept nun noch besser geschützt. Darüber hinaus lassen sich so die individuell festgelegten Zugriffsregelungen und Rechte überwachen sowie die Einhaltung des Vier-Augen-Prinzips für maximalen Datenschutz gewährleisten.

Einblick ins ARTEC-Angebot

Fazit

Ob Verschlüsselung, Dokumenten- und Informationsmanagement, Authentifizierung oder Firewalls – das Security-Angebot bei sysob ist dank vieler Partner ausgewogen und vielseitig. Die Produkte decken zahlreiche Schwachstellen ab und gewährleisten die Sicherheit von Geräten, Daten und geistigem Eigentum. Kopflos sämtliche Lösungen anzuschaffen ist dennoch nicht ratsam. Die Folgen sind oftmals unzureichende Absicherungen, Fehlinvestitionen und gestresste IT-Teams, die an zu vielen „Baustellen" gleichzeitig arbeiten müssen. Wenn Sie Hilfe bei der Planung eines adäquaten Konzepts brauchen, Interesse an den vorgestellten Produkten oder Fragen zum Thema Cybersecurity haben, stehen Ihnen unsere Produktmanager gerne zur Verfügung.

Sprechen Sie mit uns!

Unsere Kontaktdaten:

sysob IT-Distribution GmbH & Co. KG
Kirchplatz 1
93489 Schorndorf

Telefon: +49 (0) 9467/7406-0
Telefax: +49 (0) 9467/7406-290
E-Mail: info@sysob.com
http://www.sysob.com