Next-Generation Firewalls NGFW und Cloud Security

Segmentierung von Netzsegmenten On-Premise, in der Cloud sowie erweiterte Sicherheitsfunktionen (Next-Generation Firewall & UTM) und Cloud Workloud Protection

Segmentierung **von Netzwerken**

Die Trennung von Netzwerken gehörte schon immer zur Kernaufgabe von Firewall-Systemen. Allerdings ist die Firewall schon längst nicht mehr als Burgmauer zu verstehen, die auf Port-Ebene eine Verbindung vom Internetz zu einem internen Netz zulässt oder eben verhindert.

Netztrennung hilft Risiko zu minimieren

Heutzutage gibt es keine klaren Netzwerkgrenzen mehr. Auch die Trennung von Produktions- und Office-Netzwerken sowie eine mögliche Microsegmentierung z. B. in Operational Technology (OT) Netzwerken gehört zur Aufgabe von Next-Generation Firewall-Systemen (NGFW).

Moderne NG-Firewall-Systeme übernehmen weitere Aufgabenstellungen wie beispielsweise die Überwachung von Applikationen oder auch die Erkennung von Malware.

Applikationssicherheit

Applikationssicherheit / Application Control sind Teil eines Firewall-Konzepts, welches es ermöglicht, Anwendungen und Bedrohungen unabhängig von den Netzwerkprotokollen zu erkennen. So werden legitime von nicht gewünschten Verbindungen unterschieden und Angriffe unterbunden.

Web Sicherheit

Durch die steigende Nutzung wachsen auch die Anforderungen an die zentralen Übergänge und einen performanten und virenfreien Internet-Zugriff zu ermöglichen. Gleichzeitig wird die Umsetzung der klassischen Proxy- Struktur erschwert, da immer mehr Zugriffe verschlüsselt erfolgen.

Eine moderne Security-Architektur bedeutet in vielen Fällen mehr Flexibilität und Sicherheit, einfachere Handhabung und weniger Investitionskosten als mehrere Einzellösungen.

Cloud Security

Security-Funktionalitäten können von dedizierte HW-Appliances oder von virtuellen Systemen bereitgestellt werden. Ebenso können diese als Security-Service wie Secure Mail- oder Web aus der Cloud bezogen werden.

Security aus und für die Cloud

Bei dem Schutz der Cloud gilt es die Daten, die in Privat-, Public-, oder Hybrid-Clouds abgelegt werden, oder Services welche in der Cloud bereitgestellt werden, ebenso zuverlässig zu schützen wie bei On-Premise Architekturen. Gleichzeitig muss gewährleistet sein, dass die agile Nutzung von Cloud-Ressourcen nicht durch Security-Anforderungen eingeschränkt wird.

Information Security

Controlware Security-Portfolio

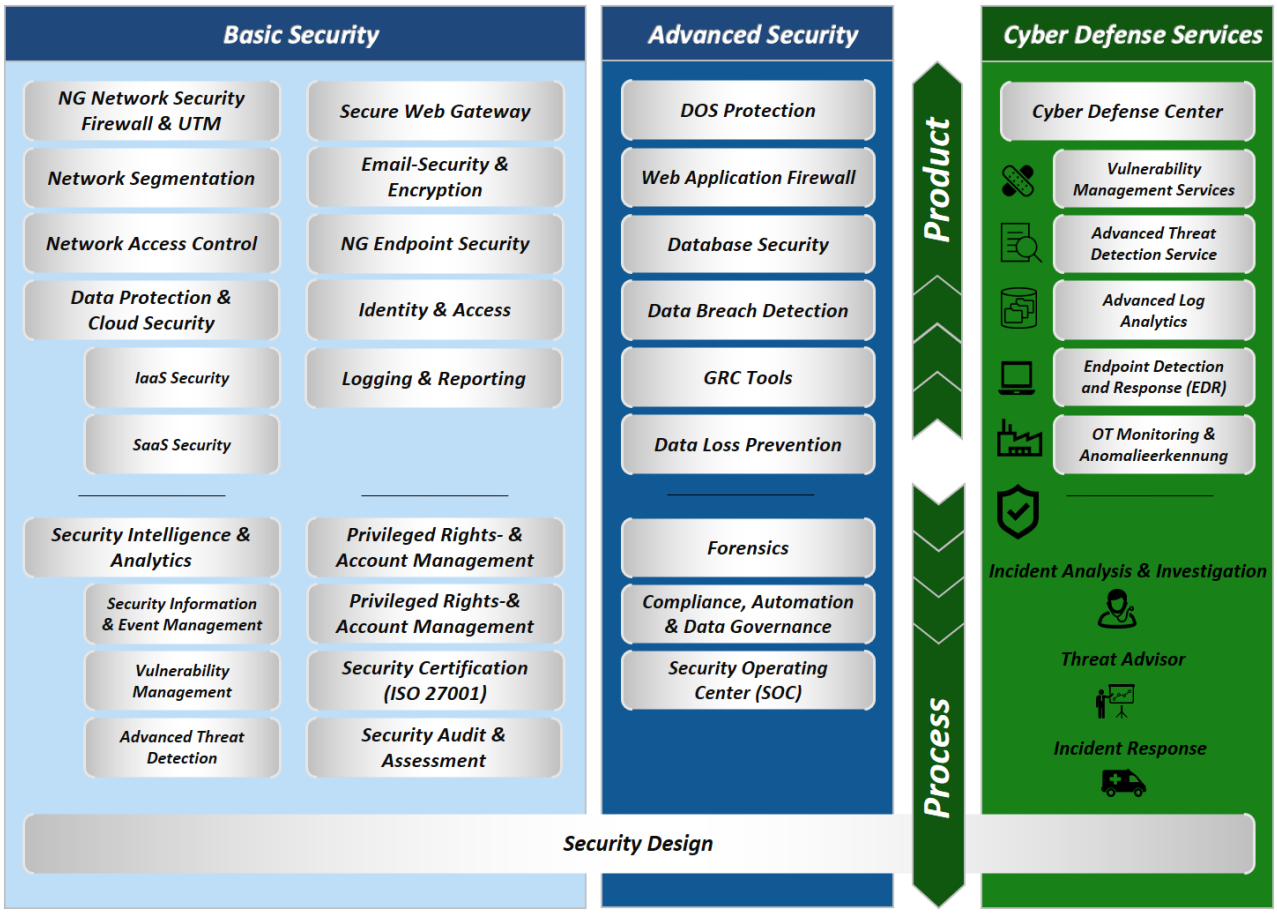
Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Ein vernünftiger Informationsschutz sowie die Grundsicherung von IT und OT sind schon mit verhältnismäßig geringen Mitteln zu erreichen. Informationssicherheit sollte allerdings als laufender Prozess mit Risikoanalyse und Prozessoptimierung verstanden werden um zielgerichtet und möglichst wirtschaftlich in ein Unternehmen oder eine Behörde integriert zu werden.

Die Kombination unserer langjährigen Expertise (Controlware Security seit 1996) mit marktführenden Anbietern von Security-Lösungen steht für erfolgreiche Projekte.

Zusätzlich verschafft uns der höchste Partnerstatus von Controlware bei nahezu allen unseren etablierten Hersteller-Partnern zahlreiche Vorteile, die wir gerne an Sie weitergeben.

Selbstverständlich können Sie auch bei Audits und Zertifizierungen gemäß national und international anerkannter Standards wie ISO 27001, ISO27001 auf Basis IT-Grundschutz / Cobit auf uns bauen.

Mit unseren Controlware Cyber Defense Services erhalten Sie für Ihr Unternehmen modular passende Security Services und mit konkreten Handlungsempfehlungen von unseren erfahrenen Analysten, die zu Ihrer Infrastruktur passen.



Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108
info@controlware.de
www.controlware.de