Web Application Firewalls

– Schutz vor Hackerangriffen, Datendiebstahl und Ausfällen

Datendiebstahl und die Verbreitung von Malware über Internet-Seiten, Online-Shops und Sozial-Media-Seiten sind auch heute noch die größten Gefahren vor denen sich Betreiber von Internet Seiten schützen müssen.

Dynamische Denial-of-Service-Angriffe (DDoS) sowohl auf einzelne Anwendungen wie auch auf die gesamte Unternehmensinfrastruktur nehmen ebenfalls zu. Die Kosten für Ausfälle gehen bei den Unternehmen in die Millionen.

Es ist es wichtig, dass innovative Systeme zum Einsatz kommen, welche immer „up to date“ sind um vor den aktuellsten Gefahren zu schützen.

Inzwischen werden WAF Firewalls als hybride Modelle zusammen mit DDoS Schutzmechanismen angeboten, da einige WAF Angriffe auf die Verfügbarkeit von Services abzielen und nicht auf den unautorisierten Zugriff von sensiblen Daten.

Grundsätzlich sollten Web-Anwendungen bereits in der Design- und Entwicklungsphase abgesichert werden. Doch selbst bei vermeintlich sicheren Entwicklungen sind Fehler bzw. Schwachstellen nie völlig auszuschließen.

Herkömmliche Security Gateway Lösungen sind nicht in der Lage Web Applikationen vor Hackern zu schützen, denn es findet auf diesen Systemen keine Analyse des übertragenen Codes statt. Diese spezifische Funktion übernehmen Web Application Firewalls (WAF).

Eine WAF wird meist inline betrieben und prüft den Traffic auf ungefährliche und gefährliche http und https-Anfragen hin. Erst wenn diese Prüfung positiv (kein Angriff) ausgefallen ist, werden die Daten zum Webserver weitergeleitet. Dieses Grundprinzip gilt für alle Arten von WAFs; jede Art filtert die http-Anfragen, bevor diese weiter zum Server geleitet werden.

Web Application Firewalls bieten Ihnen:

- Schutz sensibler Kunden- und Datenbank-informationen
- Schutz der Daten vor Diebstahl, zum Beispiel von Bank- und Kreditkarten Informationen.
- Hohe Verfügbarkeit des Online-Geschäftes
- Verfügbarkeit von Webseiten und Web-Services, z. B. durch die Abwehr von Denial-of-Services-Attacken auf Layer 7 und Vermeidung von Cross-Site-Scripting.
- Erhöhte Sicherheit
- Die Integration einer WAF–Lösung ist genauer als "Deep Inspection" klassischer Firewalls und erweitert eventuell schon vorhandene IPS.
- Schutz vor Imageverlust
- Bewahrung der Integrität von Web-Inhalten durch die Vermeidung von Web-Defacing (Veränderungen auf der Webseite)

Controlware Security-Portfolio

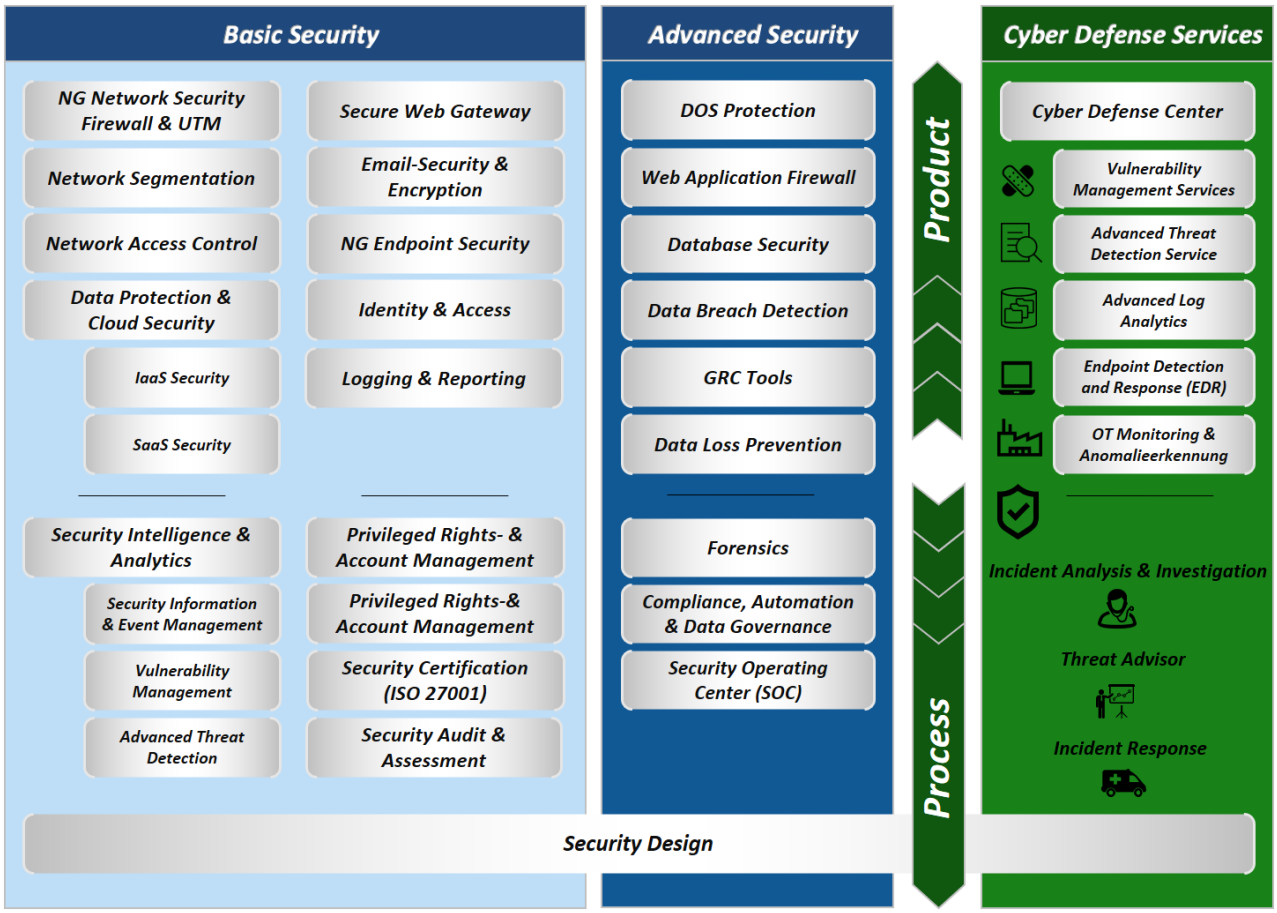
Informationen sind ein wesentlicher Wert für Unternehmen und Behörden und müssen daher angemessen geschützt werden. Ein vernünftiger Informationsschutz sowie die Grundsicherung von IT und OT sind schon mit verhältnismäßig geringen Mitteln zu erreichen. Informationssicherheit sollte allerdings als laufender 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