Secure Content Management

Email-Sicherheit, Web-Gateway, Endpoint-Schutz

Malware zu Gast in Ihrem Netzwerk?

Pausenlos sind Netzwerke und Arbeitsplätze der Bedrohung durch Malware ausgesetzt. Schon ein falscher Klick kann verheerende Folgen haben: IT-Systeme werden infiziert und von außen angreifbar; Unternehmensdaten geraten in falsche Hände; ganze Netzwerke liegen lahm.

Abgesehen vom Verlust von Daten und dem Zeitaufwand für die Wiederherstellung, schädigen solche System-ausfälle nachhaltig das Ansehen des Unternehmens.

Malware in der historischen Form

Email Sicherheit

Ganz gleich, ob es sich um eine integrierte Lösung, eine komplexe Mail-Security-Architektur oder einen ausgelagerten Managed-Mail-Service handelt – versierte Controlware-Spezialisten erarbeiten mit Ihnen eine Lösung, die speziell auf Ihre Bedürfnisse zugeschnitten ist.

Ergänzende Dienstleistungen aus dem Bereich Consulting sowie Workshops und Audits unterstützen Sie beim Erstellen einer Policy und bei der Realisierung des Projektes. Unsere Operating- und Care-Services runden das Portfolio ab.

AntiSpam	Filterung aller Spam-Mails
Threat Detection	Malware-Protection mit optionaler Sandbox für Zero Day Angriffe
URL-Check	Live Check von eingebetteten URL-Links
Encryption	Optionale Verschlüsselung der Inhalte
Archivierung	Gesetzliche Vorgaben erfüllen

Web Sicherheit

Durch die steigende Digitalisierung von Geschäfts-prozessen und die vermehrte SaaS-Nutzung wachsen auch die Anforderungen an einen performanten und virenfreien Internet-Zugang. Gleichzeitig wird die Umsetzung der klassischen Proxy- Struktur erschwert, da immer mehr Zugriffe verschlüsselt erfolgen und daher sollte neben der Evaluierung einer neuen Lösung auch vorab die firmeneigene Internet-Security-Policy über-arbeitet werden.

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

Je nach Kundenanforderungen können die neuen Web-Gateway Lösungen entweder als dedizierte HW-Appliance, als virtuelles System oder als Security-Service aus der Cloud bezogen werden. Im Idealfall gibt es nur eine Management-Konsole, die die Policy über alle Instanzen hinweg festlegt und Log- und Audit-Daten zentral sammelt und über eine Schnittstelle dem SOC-Team in Echtzeit zugänglich macht.

Im Rahmen des Controlware Web-Assessments nehmen wir Ihren Internet-Traffic unter die Lupe, ohne in den aktiven Datenverkehr einzugreifen. Innerhalb weniger Tage liefern wir Ihnen einen detaillierten, auf User-Ebene anonymisierten Report über das Gefahren-Potential der Internet-Nutzung in Ihrem Unternehmen.

Typische Web Gateway Funktionen sind hierbei:

Web-Proxy	Übernimmt Authentisierung und URL-Filterung sowie Malware-Erkennung
Ad.Threat Defense	Optionale erweiterte Malware-Erkennung für Zero-Day-Angriffe
SSL-Interception	Kontrolle von verschlüsseltem Traffic
CASB	Darstellung u. Risiko-Bewertung der genutzten SaaS-Services
Web-Isolation	Optionale Erweiterung für exponierte User und sensible Abteilungen
SD-WAN	Integrierte SD-WAN-Steuerung bei Cloud-Proxy-Services
DNS-Security	Erweiterte Kontrolle von DNS-Traffic nach Anomalien
Firewalling	Integrierte Firewalling oder IPS-Funktion für Außenstellen im SaaS-Service
Remote VPN	Optionale Erweiterung bei SaaS für den Zugriff auf firmeneigene Applikationen in der Cloud oder im DataCenter

Workplace Protection

Die Vielfalt an Endgeräten hat weiterhin zugenommen und trotz der Marktposition von MS Windows im Firmenumfeld sind für eine firmenweite Strategie auch die mobilen Geräte wie Tablets und Smartphones mit zu berücksichtigen.

Ältere Lösungsansätze haben sich sehr stark auf den Aspekt „Protection“ konzentriert und dazu Antimalware und Verschlüsselung sowie Firewalling und Port-Kontrolle in einer Suite gebündelt. In letzter Zeit wurde die Malware-Erkennung oft durch Einführung von Verhaltensanalyse oder Machine Learning Komponenten verbessert.

Heute bieten viele Hersteller eine „Plattform-Unterstützung“, wo auch der Endpoint von einer zentral bereitgestellten Sandbox partizipieren kann.

Allerdings sind damit die klassischen Suiten teilweise sehr stark gewachsen und belasten zunehmend die Rechenleistung. Kunden hingegen wünschen sich vermehrt eine stärkere Unterstützung bei der Erkennung von unbekannten Angriffen (Detection) und konkrete Hilfestellung bei der Beseitigung (Response).

Neue Lösungsideen setzen daher auf einen einfachen Grundschutz z. B. dank Microsoft Defender und der Anreicherung durch einen kleinen EDR-Agenten.

Endpoint Detection und Response Tools helfen, den Arbeitsplatz gegen Anomalien und Zero-Day-Angriffen zu schützen. Um den Mehrwert im Alltag nutzen zu können, sind allerdings die eigenen Mitarbeiter zu schulen oder alternativ sich Hilfe über einen Managed EDR Service zu besorgen.

Workplace Protection kann je nach den Kundenanforderungen und Gerätetypen folgendes umfassen:

AntiMalware	Sinnvoller Antiviren-Grundschutz gegen bekannte Viren
Application Control	Nur vorab zugelassene Applikationen / Prozesse können gestartet werden
Firewall / HIPS	Absicherung von ein- und ausgehendem Verkehr
USB-Port	Reglementierung auf firmeneigene Devices
Machine Learning	Zusatzmodul zur Erkennung von modifiziertem Schadecode
Sandbox	Optionale Anbindung an zentrale Sandbox-Komponenten
MDF	Mobile Device Management
EDR	Endpoint Detection & Response – oft der erste Wunsch von CISCO oder SOC-Teams
Managed EDR Service	Externe Unterstützung bei Analyse und Beseitigung von Schadecode

Zentrale

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