CRITICALSTART

SECCON 2
REFERENCE ARCHITECTURE

THE DEFENDABLE NETWORK

MPLS/SD-WAN Connected Networks

Web Proxy
Web Proxy to control outbound web traffic

DLP Sensor
Inspect all outbound traffic for DLP violations

IDS/IPS
Inspect all inbound/outbound traffic for anomalous or known malicious activity.

Gateway Firewall
Layer 7 Firewall configured for least permissive access. All traffic logged. User-based access control to IT resources.

Remote

Remote Workstations

Mobile devices

MFA required for access to externally facing company resources and VPN

Network traffic for managed systems off the network is monitored/restricted

Only mobile devices managed by MDM are allowed to access resources externally

WAF

WAF

All switches should have port security enabled with NAC device posture checking and MFA required for networks access.

Network should be physically separate with a separate Internet connection or at a minimum segmented by a firewall from the internal network

DMZ Web Subnet

Internal Web Subnet

Logs sent to SIEM

Internal App Subnet

Workstations

Client Subnet

IoT Subnet

Internal Wireless Subnet

Guest Subnet

DMZ App Subnet

Internal DB Subnet

Separate subnets for each individual, business unit, dept. or common access IT resources access requirements

Advanced malware/exploit protection EDR and DLP software installed on all workstations

MFA authentication required. Computer or company issued certificate and user credential required for access.

Access limited to authorized security personnel

DMZ DB Subnet

Internal Infra. Subnet

System and security logs sent to SIEM

AD/DNS

DNS, DHCP, System and Security logs sent to SIEM

Email

System, network and application activities should be logged for all business critical asstes or assets that handle sensitive / confidential information

SIEM Security Management Subnet

Micro segmentation
A least privileged security model should be enforced on all assets deemed business critical and/or assets that process or information deemed sensitive or confidential in nature. This is typically done through virtualization and/or containerization.

All AD Authentication logs, DNS logs and policy change logs sent to SIEM

All inbound email scanned for threats. All outbound email inspected for DLP violation. All logs sent to SIEM.

SIEM deployed to centralize storage of all security logs for analysis.

Vulnerability Mgmt.
All host routinely scanned for vulnerabilities and process in place to remediate identified vulnerabilities.

PAM
PAM (Privileged account management) deployed to manage / monitor privileged access to resources.

EDR Mgmt.
Advanced Threat Detection / EDR software installed on all systems. Logs configured to go to SIEM

TIP
(Threat Intelligence Platform) External threat intelligence sources should be used to enrich data and identify potentially known malicious traffic patterns.

Next-Gen AV Server
Next-Gen Antivirus server to detect/ prevent malware, exploit attempts and malicious scripts from running on endpoints

Assets Management Database
Comprehensive list of all company IT assets with primary user and team responsible for administrative management recorded. CMDB with all changes to critical assets logged in accordance with the change management process

MDM
MDM (Mobile Device Management) server to manage / validate security configurations of supported mobile devices

CC BY SA