SMB External Attack Surface (EAS) Best Practice

Executive Summary

This document provides small business owners with essential best practices to minimize their external attack surface, covering vulnerabilities in web applications, cloud services, and network configurations. By addressing issues like exposed APIs, misconfigured DNS, and unpatched remote access points, SMBs can significantly reduce their risk of cyberattacks and protect sensitive data.

Public-Facing Web Servers & Applications

SecurityScorecard factor(s): Application Security + Network Security

- **Vulnerabilities in public-facing Web Applications:** SMBs websites and web applications that may have vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). These can be exploited to gain unauthorized access or inject malicious code.
- **Exposed APIs:** Many SMBs expose APIs for their services (e.g., customer portals, mobile apps). Improperly secured APIs with weak authentication or authorization controls can provide attackers with direct access to sensitive data.
- **Outdated Web Frameworks/Plugins:** Many SMBs use third-party plugins, frameworks, or content management systems (CMS) like WordPress, Joomla, or Magento. If these are outdated, they may contain known vulnerabilities that attackers can exploit.
- **SSL/TLS Misconfigurations:** Poor SSL/TLS configurations, such as using weak ciphers, unpatched vulnerabilities, or improperly installed certificates, can expose sensitive data to man-in-the-middle (MITM) attacks.

DNS and Domain Misconfigurations

SecurityScorecard factor(s): DNS Health & IP Reputation

- **DNS Zone Transfers:** Poorly configured DNS servers may allow attackers to perform zone transfers and retrieve sensitive domain-related information (e.g., subdomains, internal IP addresses) that can aid in further attacks.
- **Subdomain Takeover:** If an SMB abandons a subdomain or an associated service, attackers can register that subdomain and exploit it for malicious purposes, including phishing, malware delivery, or hosting fake services.
- **DNS Spoofing/Cache Poisoning:** Attackers can target DNS servers to alter the resolution of domains, redirecting users to malicious websites. This is often done by compromising the DNS cache or through man-in-the-middle attacks.

Email Server Exposure

SecurityScorecard factor(s): DNS Health

- **Open Email Relays:** Misconfigured email servers may allow attackers to send spam or phishing emails from the domain of the SMB. Open relays can be exploited by cybercriminals to conduct mass phishing campaigns.
- **SPF/DKIM/DMARC Misconfigurations:** Failure to implement or incorrectly configuring SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance) can lead to email spoofing and phishing attacks.

Cloud Services Misconfigurations

SecurityScorecard factor(s): Network Security

- **Exposed Cloud Storage:** Improper configuration of cloud storage services like AWS S3, Google Cloud Storage, or Azure Blob Storage can lead to data being publicly accessible. Common misconfigurations include public read/write permissions or lack of access control lists (ACLs).
- **Unprotected Cloud Databases:** Cloud-based databases (e.g., AWS RDS, MongoDB, or PostgreSQL) left exposed to the internet can be easily exploited if not properly secured (e.g., default passwords or open ports).

Firewall and Network Perimeter Issues

- **Open Ports:** Many SMBs fail to close unnecessary open ports on their firewall, exposing services (such as databases, management consoles, or administrative interfaces) to the internet, which can then be exploited by attackers.
- **Exposed Internal Services:** Sometimes internal services or servers are unintentionally exposed to the public internet, which can provide attackers with an entry point into the internal network.

Remote Access Points (VPNs, RDP, etc.)

SecurityScorecard factor(s): Patching Cadence + Network Security

- **Unpatched VPN Servers:** If the SMB provides remote access via VPNs, unpatched or misconfigured VPN servers could allow attackers to gain access to the internal network. Common vulnerabilities include weak authentication, outdated VPN protocols, and missing patches.
- **RDP (Remote Desktop Protocol) Exposure:** Many SMBs use RDP for remote access. Exposing RDP directly to the internet, especially without multi-factor authentication (MFA), makes it an attractive target for brute-force attacks and credential stuffing.
- **Weak Authentication or No MFA:** Remote access points (VPN, RDP, SSH) often lack proper authentication mechanisms or multi-factor authentication, leaving them vulnerable to credential theft or brute-force attacks.

Publicly Accessible SSH, Telnet, FTP, and other Services

SecurityScorecard factor(s): Network Security

- **Weak SSH Keys:** SSH keys that are weak (e.g., using small key sizes or default keys) or not properly rotated can be exploited by attackers to gain access to remote servers or devices.
- **Telnet Exposure:** Telnet is an unencrypted communication protocol. If exposed, it provides an attacker with the ability to intercept unencrypted credentials and commands during transmission.
- **FTP Exposure**: Exposing FTP without proper security measures allows attackers to intercept credentials and manipulate files due to its unencrypted nature.
- **Other Services**: Database and other authentication services if exposed externally can be exploited by attackers to steal data or breach defenses.

Exposed Backup Systems

- **Open Backup Ports:** Backup services that are exposed to the internet without proper protection (e.g., unencrypted communication or open ports) can become targets for attackers, who may steal or corrupt critical backup data.
- **Unsecured Backup Cloud Accounts:** Backup systems stored in the cloud can become exposed if proper security measures (like encryption, MFA, and access controls) are not implemented.

IoTs & Unmanaged Devices/Shadow IT

SecurityScorecard factor(s): Patching Cadence + Network Security

- **Unpatched IoT Devices:** Many SMBs deploy Internet of Things (IoT) devices such as printers, cameras, or smart thermostats. If these devices are not properly patched or secured, they can be exploited to gain access to the network.
- **Default Credentials:** Many IoT devices come with default usernames and passwords that SMBs neglect to change, providing attackers with an easy way to compromise the device and gain network access.
- **BYOD Devices:** Employees' personal devices (laptops, smartphones) connected to the SMB's network may have weak security configurations or outdated software, increasing the risk of external attacks via malware or vulnerabilities.

Social Media and Digital Presence

SecurityScorecard factor(s): Hacker Chatter + Information Leak + Social Engineering

- **Information Leakage via Social Media:** Attackers may conduct social engineering or reconnaissance by gathering information from publicly available social media profiles or business directories, which can then be used for phishing or impersonation attacks.
- **Leaked data:** Information obtained from ransomware, hacked or compromised emails, other PII exposed on hacker forums or the dark web.
- **Leaked Subdomain Information:** Information about an SMB's digital infrastructure may be available through publicly accessible domain records (WHOIS) or online tools, which can assist attackers in targeting specific technologies or services.

The Hartford Insurance Group, Inc., (NYSE: HIG) operates through its subsidiaries, including underwriting company Hartford Fire Insurance Company, under the brand name, The Hartford®, and is headquartered at One Hartford Plaza, Hartford, CT 06155. For additional details, please read The Hartford's legal notice at **www.TheHartford.com**

About SecurityScorecard

SecurityScorecard helps security professionals work collaboratively to solve mission-critical, cybersecurity issues in a transparent way. The SecurityScorecard platform provides continuous, non-intrusive cyber risk monitoring of any organization and its ecosystem.

Ready to get started? Schedule a demo today: **https://securityscorecard.com/the-hartford/**