CYBER SECURITY CHECKLIST

PREVENTING INITIAL COMPROMISE

ALERT LOGIC®

ais APPLIED INFORMATION SCIENCES

PROTECTING YOUR DATA

This security overview provides best practices to help organizations looking to harden their environment. Designed to help small- to mid-sized organizations stop an attack before one starts, this basic guidance will help reduce your attack surface and outlines practical steps to securing your enterprise. With this checklist, you will have a guide to help prevent initial compromise and stop attacks before they start.

This checklist helps explain how to:

- Address software vulnerabilities and misconfigurations
- Eliminate exposed ports & services
- Reduce the chance of attacks delivered via email
- Limit browser-based attacks
- Reduce the attack surface across Microsoft Office applications

Lastly, we will share details on how AIS and Alert Logic helps organizations of all sizes get a comprehensive view of their enterprise assets, find misconfigurations and vulnerabilities, and delivers endpoint coverage with an automated quarantine response to stop malware in its tracks.

PREVENTING INITIAL COMPROMISE

The best defense against cyber attacks is to prevent attackers from gaining initial access to a machine in the first place.The organizations business strategy and goals are translated into iterative activities such as:

☐ **Prioritize Patching**

When vulnerabilities are disclosed, it's only a matter of time before attackers begin exploiting them. Having a system in place to assess, test, and roll out patches is a vital first defense against attacks.

☐ **Isolate What You Can't**

Patching is vital, but not easy and it can be impossible in some cases. Isolate systems you can't patch quickly by restricting system access.

ELIMINATE EXPOSED PORTS & SERVICES

- [ ] **Secure Remote Desktop (an RDP)**

  Open ports with RDP exposed to the Internet are beacons for attackers. Restrick access to RDP listening ports by placing them behind a firewall and using a RDP Gateway. Enabling network-level authentication and changing the default listening port (TCP 3389) is also recommended.

- [ ] **Secure Server Message Block (SMB)**

  Disable SMBv1 and use firewalls to restrict SMB network activity. WannaCry and other attacks leveraging the EternalBlue exploit have shown just how vulnerable organizations become when exposing SMB. Ideally do not allow file transfer between secured networks at all.

REDUCE THE CHANCE OF ATTACKS VIA EMAIL

- [ ] **Block Common Malicious File Attacks**

  In addition to the obvious (.EXE, .BAT), consider blocking script files (.JS, .VBS, etc.), archive files (.ZIP, .SFX, .7z), and even Office files (.DOC, .DOCX, etc.) and PDFs. Consider which file attachments you wish to block carefully to strike a balance between security and the ability to do business.

- [ ] **Conduct User Awareness Training**

  Many attacks still initially require users clicking something they shouldn't. Training and inform your endusers about attacks that rely on deception and social engineering.

LIMIT BROWSER-BASED ATTACKS

- [ ] **Utilize Ad-Blockers**

  Eliminate legitimate websites can serve as infection points thanks to malvertising.

SECURITY AT YOUR FINGERTIPS

DISABLE OLE PACKAGES

- [ ] **Enforce Stricter Macro Controls**

  Block macros in Office files downloaded from the Internet. Macros are abused to download malware and launch malicious scripts.

- [ ] **Disable "Update Automatic Links at Open" in Microsoft Word**

  This will prevent abuse of the DDE feature (now disabled by default) and similar threats.

- [ ] **Desable OLE Packages**

  Considering the long history of attackers abusing Microsoft's object linking and embedding (OLE) feature, it's best disabled when possible.

ALL OF THE ABOVE

- [ ] **Establish a system that provides visibility across your organization, monitor application and system behavior for threats, implement proactive vulnerability scanning, and deploy endpoint and anti-virus protection.**

  Patching, isolation and restricting risky activity prevents a lot of initial attack vectors from causing damage yet many attacks take place through zero-day or unknown vulnerabilities in servers and applications. Visibility of systems and the ability to monitor for unusual behavior on the endpoint, servers and in applications is critical to get early warning of attack attempts and allow you to respond accordingly.

ACHEIVE BETTER SECURITY AT OPTIMAL COST

No level of investment prevents or blocks 100% of attacks. You need to continuously identify and address breaches or gaps before they cause real damage. With limited budget and expertise, you believe this level of security is out of reach. You haven't discovered Alert Logic — managed detection and response (MDR) delivering unrivaled security value. As the industry's first MDR provider, Alert Logic's purpose-built technology and team of security experts empower you to resolve whatever threats may come. Attacks are constantly evolving and we are always watching; identifying and prioritizing what to do next. We are relentless in protecting your organization. Alert Logic — our knowledge is your advantage.

Our fully managed IT services deliver a wealth of benefits. Let's start the conversation on how we can make that happen.

Contact Us

ALERT LOGIC AND AIS, BETTER TOGETHER SECURITY SOLUTIONS

Many organizations seek out support services to offload cloud management activities, focus on strategic efforts, address specific security and compliance concerns, and reduce IT costs. Alert Logic and AIS have partnered to use Alert Logic's threat intelligence Security Operations Center (SOC) to identify, filter, and coordinate mitigation efforts. Organizations, large and small, trust AIS to protect and act when security and support situations arise. In us, they find a long-term partner and strategic advisor for all their cloud transformation needs.

AIS is not your typical Managed Services provider. With AIS as your Operations and Maintenance support team, you gain access to developers, engineers, architects, data, and security experts with enterprise experience and deep Microsoft capabilities. As a Microsoft partner since 1994 with 10 Gold Competencies, we've pioneered many Azure firsts and have services to enable and support solutions across the three Microsoft clouds: Azure, Microsoft 365, and Dynamics 365. Our teams have led cloud adoption in some of the most complex enterprise environments and modernized and managed mission-critical applications for organizations like GEICO, Army Futures Command, and more.

Whether it's operations and maintenance or custom app development, tap into AIS and Alert Logic's team of cyber threat researchers, cloud SMEs, and data analysts to help solve your most challenging problems for a fixed, predictable cost.

AIS' CUSTOM TAILORED SOLUTIONS

Flexible engagement models, with experts across diverse capability areas – a one stop shop for your cloud needs.

Identity Management

Management of identity and authentication privileges, authorization, and roles.

Security and Compliance

Monitoring, detection, and remediation of security concerns to maintain continuous audit compliance

Continuous Optimization

Optimization of cloud operations, management, maintenance, security, reporting, and cost solutions.

Managed DevOps

AIS has a long history in application development using DevOps processes to help your teams deliver secure solutions faster.

Cloud Reseller

AIS is a Cloud Solution Partner (CSP) and long-term Microsoft Partner, we can support your organization in purchasing and managing licenses, migrating/deploying cloud infrastructure, modernizing applications, and managing your cloud environment – including cost optimizations and security, from Commercial to GCC-High.

www.ais.com
Copyright © 2020, Applied Information Sciences, All Rights Reserved
11440 Commerce Park Drive, Suite 600, Reston, VA 20191
Phone (703) 860-7800
sales@ais.com