OSIbeyond

Managed Security

The security of IT systems is a critical component in IT operational management. As a Managed Technology Partner for your organization, OSIbeyond provides security oversight using a multi-step process. First, by performing a vulnerability assessment of all IT systems to identify potential risks, remediate vulnerabilities, and ensure compliance with specific regulatory policies. The vulnerability assessment provides a benchmark of an organization's security situation, and is intended to be a form of self-audit that is repeated periodically. Second, by providing ongoing proactive and preventative security protection through the Enhanced Security Services designed to deliver a holistic approach by adding multiple layers of security to an organization's technology systems.

Vulnerability Assessment

Scanning

OSIbeyond conducts comprehensive scanning of your environment consisting of several key components. First, a scan of your entire network to discover and inventory all assets, including their OS, applications, and services. This is an important step to identify all assets before assessment and management of any risks that are present. Additionally, internal vulnerability scanning assesses the security of your network from inside the firewall, while external scanning is performed remotely from the outside. Performing both internal and external scanning provides a complete view of your organization's risks.

The scan also provides a unified vulnerability and configuration assessment in a single report to provide a complete view of your security risk and compliance posture. Finally, deep scanning using credentials to authenticate against assets gives you greater visibility into risks and provides additional information such as application level inventory. In contrast, anonymous scanning only provides an outsider's view of assets. Authenticated scans provide the ability to assess a wide range of OS, database, network, and application layer configurations.

Prioritization & Remediation

Once the network vulnerability scanning is complete it is important to effectively prioritize identified risks as well as implementing the proper remediation plan. Vulnerabilities can reach thousands or possibly millions in some organizations, therefore a granular risk score is provided that considers threat intelligence and temporal metrics. The risk score incorporates threat metrics such as exposure to exploits and malware kits, and how long the vulnerability has been available.

After risks are identified and prioritized, proper action must be taken to resolve them. An efficient remediation workflow is provided to create a plan for the top steps to reduce overall risk. This includes the actions required in language that the person performing the remediation will understand, time required for completion, and related patches, downloads, and references.

Reporting

Vulnerability scans can produce an overwhelming amount of information so it's important to be able to identify what is relevant, and present it in a clear, concise, and actionable format. By providing consolidated reporting using aggregated data collected from every scan, OSIbeyond ensures the ability to easily manage the prioritization, remediation, as well as analysis of security risks and compliance trends. In addition, information such as vulnerabilities, configurations, policy compliance, and other asset information including installed applications is provided in a single report. Finally, reports are prepared to meet a variety of users' needs, such as an executive level report to show the risk posture across the entire organization and IT operation level reports to detail remediation steps.

Compliance & Configuration Assessment

Vulnerability assessments are a key requirement for many security standards and regulations, such as Payment Card Industry Data Security Standards (PCI DSS). OSIbeyond can tailor the vulnerability assessment to specific industry compliance requirements. While OSIbeyond does not provide compliance certification, the vulnerability assessment provides a report assessing your organization against a specific set of compliance requirements. This reporting in conjunction with remediation steps is critical when preparing for an upcoming audit or certification.

Ensuring your systems are configured securely according to industry benchmarks and best practices is a critical component in a unified security assessment. Configuration and compliance assessments are performed at the same time as vulnerability scanning with the results presented in a unified report. In addition, configuration policies can be fully customized to meet your specific requirements.

Enhanced Security Services

The Enhanced Security Services consist of various proactive technology solutions designed to protect and prevent malicious attacks, data compromises, and vulnerabilities. The Enhanced Security Services delivers a holistic approach by adding multiple layers of security to an organization's technology systems, including email communications, user authentication, and mobile devices. The Enhanced Security Services is offered as a subscription service based on the number of users.

As cyber threats become more widespread and sophisticated, organizations can no longer ignore these risks. As demonstrated by many high profile cyber-attacks (Sony, OPM, Target, Anthem BCBS, Home Depot etc.) a cyber breach can have devastating impact to an organization including damage of customer/member trust, reputation, and direct financial losses. Cyber security is now an essential component of an organization's technology operations.

The Enhanced Security Services utilizes various tools to proactively respond, protect, and prevent attacks and breaches in four key areas.

1. Targeted Threat Protection

- **URL Protect** rewrites URLs in all inbound email. When clicked, the destination website is scanned in real-time for potential risks before being opened in the employee's browser. If the site is safe, it opens as normal. If not, a warning page is displayed and access to the website is blocked.
- **Attachment Protect** reduces the threat from weaponized or malware-¬laden attachments used in spear phishing and other advanced attacks. It includes pre-emptive sandboxing to automatically security check email attachments before they are delivered to employees. Attachments are opened in a virtual environment or sandbox, isolated from the corporate email system, security checked and passed on to the employee only if clean
- **Impersonation Protect** offers instant and comprehensive protection from the latest malware-less social engineering attacks, often called CEO fraud, whaling or business email compromise, by identifying combinations of key indicators in an email to determine if the content is likely to be suspicious, even in the absence of a URL or attachment.

2. Two factor Authentication

Two-factor authentication adds a second layer of security to your online accounts. Verifying your identity using a second factor (like your phone or other mobile device) prevents anyone but you from logging in, even if they know your password.

Passwords are increasingly easy to compromise. They can often be stolen, guessed, or hacked, you might not even know someone is accessing your account. Two-factor authentication adds a second layer of security, keeping your account secure even if your password is compromised. With Push notification, you'll be alerted right away (on your phone) if someone is trying to log in as you. This second factor of authentication is separate and independent from your username and password.

3. Mobile Device Security

Mobile Device Security provides centralized management of smartphones and tablets, to help safeguard devices and data. Mobile Device Security includes the following compliance and security features:

- Set granular security policies for specific devices or persona policies that span across devices.
- Specify passcode policies and encryption settings.
- Detect and restrict jailbroken and rooted devices.
- Remotely locate, lock and wipe lost or stolen devices; selectively wipe corporate data while leaving personal data intact.
- Create near real-time compliance rules with automated actions.

4. Phishing Security Tests

OSIbeyond conducts automated monthly employee Phishing Security Tests (PST). The Phishing Reply Tracking allows you to track if a user replies to a simulated phishing email and can capture the information sent in the reply. You can also track links clicked by users as well as test and track if users are opening Office attachments and then enabling macros.

In case an employee falls for one of the simulated phishing attacks, you have several options for correction, including instant remedial online training. The scheduled monthly simulated phishing attacks are highly effective and immediately allow you to see which employees fall for these social engineering attacks.

Interested in Learning More?

Contact Us