African Cyber Security

BEST PRACTICE GUIDELINES FOR BUSINESSES

Employ Defense-in-Depth Strategies

Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls as well as gateway antivirus, intrusion detection or protection systems (IPS), website vulnerability with malware protection, and web security gateway solutions throughout the network.

Monitor for Network Incursion Attempts, Vulnerabilities, and Brand Abuse

Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious website reporting.

Antivirus on Endpoints Is Not Enough

On endpoints, it is important to have the latest versions of antivirus software installed. Deploy and use a comprehensive endpoint security product that includes additional layers of protection, including:

- Endpoint intrusion prevention that protects unpatched vulnerabilities from being exploited, protects against social engineering attacks, and stops malware from reaching endpoints.
- Browser protection for avoiding obfuscated web-based attacks.
- File and web-based reputation solutions that provide a risk-and-reputation rating of any application and website to prevent rapidly mutating and polymorphic malware.
- Behavioral prevention capabilities that look at the behavior of applications and prevent malware.
- Application control settings that can prevent applications and browser plugins from downloading unauthorized malicious content.
- Device control settings that prevent and limit the types of USB devices to be used.

Secure Websites Against Attacks and Malware Infection

Avoid compromising your trusted relationship with customers by regularly assessing your website for vulnerabilities and malware. Additionally, consider:

- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users.
- Displaying recognized trust marks in highly visible locations on your website to show customers your commitment to their security.

Protect Private Keys

Make sure to get your digital certificates from an established, trustworthy certificate authority that demonstrates excellent security practices. Symantec recommends that organizations:

- Use separate Test Signing and Release Signing infrastructures.
- Secure keys in secure, tamper-proof, cryptographic hardware devices.
- Implement physical security to protect your assets from theft.

Use Encryption and DLP to Protect Sensitive Data

Implement and enforce a security policy whereby any sensitive data is encrypted. Ensure that customer data is encrypted as well. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization.

Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution that can help prevent data breaches and minimize their impact.

- Implement a DLP solution that can discover where sensitive data resides, monitor its use, and protect it from loss.
- Monitor the flow of information as it leaves the organization over the network, and monitor traffic to external devices or websites.
- DLP should be configured to identify and block suspicious copying or downloading of sensitive data.
- DLP should also be used to identify confidential or sensitive data assets on network file systems and computers.

African Cyber Security

BEST PRACTICE GUIDELINES FOR BUSINESSES

Ensure All Devices Allowed on Company Networks Have Adequate Security Protections

If a bring-your-own-device (BYOD) policy is in place, ensure a minimal security profile is established for any devices that are allowed access to the network.

Implement a Removable Media Policy

Where practical, restrict unauthorized devices, such as external portable hard-drives and other removable media. Such devices can both introduce malware and facilitate intellectual property breaches, whether intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

Be Aggressive in Updating and Patching

Update, patch, and migrate from outdated and insecure browsers, applications, and browser plugins. This also applies to operating systems, not just across computers, but mobile, ICS, and IoT devices as well. Keep virus and intrusion prevention definitions at the latest available versions using vendors' automatic updates.

Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

Enforce an Effective Password Policy

Ensure passwords are strong. Passwords should be at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple websites and sharing passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days.

Ensure Regular Backups Are Available

Create and maintain regular backups of critical systems, as well as endpoints. In the event of a security or data emergency, backups should be easily accessible to minimize downtime of services and employee productivity.

Restrict Email Attachments

Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments. Ensure that mail servers are adequately protected by security software and that email is thoroughly scanned.

Ensure Infection and Incident Response Procedures Are in Place

- Keep your security vendor contact information handy; know who you will call, and what steps you will take if you have one or more infected systems.
- Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss.
- Make use of post-infection detection capabilities from web gateway, endpoint security solutions and firewalls to identify infected systems.
- Isolate infected computers to prevent the risk of further infection within the organization, and restore using trusted backup media.
- If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied.

Educate Employees

As ever, basic common sense and the introduction of good security habits can go a long way to keeping sites and servers safe this year.

- Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless from a trusted source or the download has been scanned for malware.
- Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends.
- Deploy web browser URL reputation plugin solutions that display the reputation of websites from searches.
- Restrict software to corporate-approved applications, if possible, and avoid downloading software from file sharing sites. Only download packages directly from trusted vendors' websites.

BEST PRACTICE GUIDELINES FOR BUSINESSES

- Educate users on safe social media conduct. Offers that look too good usually are, and hot topics are prime bait for scams. Not all links lead to real login pages.
- Encourage them to adopt two-step authentication on any website or app that offers it.
- Ensure they have different passwords for every email account, applications and login—especially for work-related sites and services.
- Remind then to use common sense. Having antivirus and security software doesn't mean it is ok to visit malicious or questionable websites.
- Encourage employees to raise the alarm if they see anything suspicious. For example, if Windows users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (indicative of fake antivirus infections), educate users to close or quit the browser using Alt-F4, CTRL+W or to use the task manager, and then notify the helpdesk.

Protect Mobile Devices

We recommend that people and employers treat mobile devices like the small, powerful computers that they are and protect them accordingly using:

- Access control, including biometrics where possible.
- Data loss prevention, such as on-device encryption.
- Automated device backup.
- Remote find and wipe.
- Regular updating. For example, the latest version of Android, codenamed 'Honeycomb', includes a number of features designed specifically to thwart attackers.
- Common sense. Don't jailbreak devices and only use trusted app markets.
- Training, particularly around paying attention to permissions requested by an app.
- Security solutions such as Symantec Mobility or Norton Mobile Security

We have seen the number of mobile vulnerabilities increase every year over the past three years—although this is perhaps an indicator of progress rather than a cause for despair. It is an indication that security researchers, operating system developers and app writers are, in fact, paying more attention to mobile security by identifying and fixing more problems.

Although we expect mobile devices to come under growing attack over the next year, there is also hope that with the right preventative measures and continuing investment in security, users can achieve a high level of protection against them.

Building Security into Devices

The diverse nature of ICS and IoT platforms make host-based intrusion detection systems (IDS) and intrusion prevention systems (IPS), with customizable rulesets and policies that are unique to a platform and application, suitable solutions.

However, manufacturers of ICS and IoT devices are largely responsible for ensuring that security is built into the devices before shipping.

Building security directly into the software and applications that run on the ICS and IoT devices should prevent many attacks that manage to side-step defenses at the upper layers. Manufacturers should adopt and integrate such principles into their software development processes.

Business users and consumers need to be assured that suppliers are fundamentally building security into the IoT devices that they are buying, rather than it being considered as a bolt-on option.

It's a Team Effort

Consumer confidence is built up over multiple interactions across numerous websites owned by countless different organizations. But it only takes one bad experience of stolen data or a drive-by download to tarnish the reputation of every website in the consumer's mind.

As we said at the start of the report, there is a real opportunity in the coming year to reduce the number of successful web attacks and limit the risks websites potentially pose to consumers, but it will take commitment and action from website owners for it to become a reality.

Adopt Complete Website Security in 2016, and together with Symantec, make it a good year for cyber security and a very bad one for cyber criminals. ■