Akouto

BUSINESS TECHNOLOGY BRIEF

Cyber Security Intelligence for your business

IN THIS ISSUE

The top causes of malware infections and what you can do to keep your business safe.

PLUS

A practical checklist you can follow to protect your business.

CONTACT US

Akouto
info@akouto.com
Tel: 1-877-707-0920
www.akouto.com

➢ TOP ATTACKS AND HOW TO STAY SAFE

1 PHISHING ATTACKS

Phishing and spear-phishing are the leading cause of malware infections and breaches.

2 EXPLOIT KITS

Hacked websites contain software that can infect vulnerable and unpatched systems.

3 MALVERTISING

Malicious ads displayed on legitimate sites can infect computers. No click required!

4 DOWNLOADS

Software downloads often contain viruses, including mobile apps you download from the app store.

TRAINING

Studies show that cyber awareness training can reduce chances of getting hacked by 70%. Access your free cyber awareness training at **akouto.com/cyber-security-101/**

BACKUPS

No matter what any vendor claims, no security measure can provide a 100% guarantee. Make sure you have backups in place so you can recover your critical data in case of a breach.

INTRUSION PREVENTION

A managed Intrusion Prevention System can prevent viruses, ransomware and other threats from impacting your business.

ANTI-VIRUS

Anti-virus is a necessary component of a sound cyber security strategy, which should include all these tools to minimize business risk.

Follow this practical guide to make sure you are taking the necessary steps to protect your business from costly malware infections and security breaches.

Recommendations

The six remediation areas and specific recommendations provided in this security brief are based on the latest online threats. Businesses are encouraged to take the following measures to prevent downtime and costly repairs caused by viruses, ransomware and security breaches:

1. **Update software and patch IT infrastructure**
2. **Reduce Internet footprint**
3. **Perform secure backups**
4. **Deploy professional anti-virus**
5. **Practice Cyber Security awareness**
6. **Engage Managed security services**

1. Update software and patch IT infrastructure

Users should check for and apply software updates provided by their vendors. This activity should be prioritized as follows:

1. Externally accessible servers
2. Firewalls and Routers exposed to the internet
3. Internal servers and personal computers
4. Other infrastructure such as security cameras or other internet-enabled devices

2. Reduce Internet footprint

Businesses often create firewall rules to allow employees, vendors or other third parties to access IT systems remotely. Firewall misconfigurations, or intentional creation of rules that are too broad in scope and allow access from anywhere on the internet is a common cause of security breaches.

Firewall rules should be reviewed and the number of systems that are exposed to the internet should be kept to a strict minimum. When network ports are forwarded to allow external access to IT systems, the rules should be restrictive and limit access only from a specific set or range of external IP addresses when possible.

3. Perform secure backups

Hackers are constantly looking for new vulnerabilities and vendors don't always have enough time to release patches in advance of the next attack. Security systems may be unable to stop attacks they are not able to detect (these are known as Zero-Day attacks).

Up-to-date backups are critical in order to quickly recover from an attack with minimal impact to business systems. Backup policies should take into consideration that infected systems with access to mounted backup drives may also encrypt backup files. This risk should be mitigated by having a backup strategy that keeps historical versions of backed up files and includes snapshots that are not accessible to systems that may become infected.

4. Deploy professional anti-virus

While zero-day attacks are an unfortunate reality, the fact is that the vast majority of breaches are caused by known vulnerabilities that professional anti-virus solutions are able to block. Commercial anti-virus software should be installed and licensed on all systems and configured

to automatically update virus definitions from the vendor. Additional security features provided by many commercial solutions like secure browsing extensions, identity theft protection and enhanced computer firewall features should be enabled on all computers.

5. Cyber Security Awareness

Studies show that the chance of a breach is reduced by up to 70% in businesses that engage in cyber security awareness training.

The method most commonly used by hackers to bypass security measures is phishing, where users are tricked into clicking on a link or opening an attachment in an email that looks like it came from a legitimate source like a customer, vendor, bank or other well-known company or website.

Computer users should take time to educate themselves on spam and phishing techniques as well as tips on how to detect them and ways to avoid falling victim. There are many free resources online such as **staysafeonline.org** that provide information and tips for businesses and individuals. Akouto also offers a free 15 minute cyber-awareness course at **akouto.com/cyber-security-101/**

6. Monitored Intrusion Prevention

Cyber threats are constantly changing as the cat-and-mouse game between cyber criminals and security vendors goes on. Monitored Intrusion Prevention helps to protect your business from lost revenue caused by downtime and to avoid the significant cost of recovering from ransomware, breaches and other attack. Every device on your network is protected and a team of trained cyber security experts monitors your systems for suspicious activity to quickly contain and eliminate threats.