Integris.

7 Top CyberSecurity Issues Banks Must Avoid

Integrisit.com

Contents

7 Top Cybersecurity Issues Banks Must Avoid

It probably comes as no surprise that banks keep records containing personal information. As a part of doing business, banks maintain records that list their members' Social Security Number, checking account, savings account, and credit card numbers. They also have home addresses, phone numbers, and other personal data that criminals can use to commit identity fraud. As such, they must take cybersecurity more seriously than most organizations.

When it comes to securing the kind of information that banks have on file, one cannot overstate how critical security is. Unfortunately, most banks lack the resources, workforce, and experience to protect their members from increas-ingly sophisticated attacks. When in doubt, hire a security focused managed service provider that can protect you from these seven cybersecurity threats.

1

Remote Access Trojans and Other Malware

Attackers use social engineering, drive-by downloads, and many other methods to install all sorts of malicious software, known as malware, on your system. One of the most dangerous forms of malware is known as a remote access trojan.

Once installed, an attacker can comb through your files, applications, and databases at will.

your files, applications, and databases at will.

Attackers use several methods to hide their activity, and without proper protections in place, this activity can go undetected for days, months, or even years. Usually, by the time you notice something is wrong, you will have a tough time estimating the amount of damage they caused.

Ideally, you should do everything you can to reduce the likelihood of hackers gaining access to your systems. That usually involves keep-ing your operating system and apps updated. Hackers are always on the lookout for banks, and other large organizations that are not properly patching their systems.

However, security patches don't always protect you from malware. Your employees can also make mistakes that unintentionally open the doors for hackers (spoilers). Notably, though, **60% of cybersecurity breaches** could have easily been prevented by a proper patch management program.

◄ **See more about this statistic from CSO Online**

With outdated apps and operating systems, you make it easy for criminals to access your data. A managed service provider with a fully developed vulnerability management and patching program can review all your applications and devices to ensure you stay up to date.

2

Threats from Third-Party Vendors

Let's assume that your bank has an IT professional who always keeps your software updated. As soon as developers or security researchers discover a vulnerability and release a patch, your IT person has it installed. How can you be sure that the patches you are installing are trustworthy, and how do you effectively evaluate your vendors and other third-party providers?

Attacks from third-party vendors, also known as supply-chain attacks, and they happen more often than you might imagine. **One study shows** that 80% of organizations can trace security breaches back to a vendor. Despite the exceptional risk, less than a quarter of organizations say that they have full visibility of their vendors' security measures.

Integris managed service includes collaborative support for your third-party solutions. You can also get a risk assessment before you adopt any third-party solutions. Only a vigilant position from experienced bank cybersecurity professionals can give you the oversight you need to manage the risk associated with vendors.

▲ **See more at CSO Online**

3

IoT-Based Attacks

Every device that you add to your network increases your attack surface. It used to be that only a limited number of devices were internet-enabled, making oversight of your infrastructure much easier to manage.

But the IoT (Internet of Things) is now a popular, convenient way for businesses and households to use a **wider range of devices**—including security cameras, electrical outlets, refrigerators, and light bulbs. How do you prepare for this new world of connected things?

▲ **Read more at threatpost.com**

Given the seriousness of bank cybersecurity, you should always be looking out for unauthorized IoT devices and doing a proper risk assessment before installing any new devices on your network.

For example, your new security cameras could have a vulnerability that opens your network to attacks, or your new Wi-Fi enables fridge may allow unauthorized devices to connect to it. Be sure that you are using trusted vendors, and make sure that you are aware of how your new devices could expose you to additional risk.

A reliable managed service provider can ensure that you only use trustworthy devices and installation professionals. Without that oversight, every device represents a potential unknown risk to your security.

4

Privilege Escalation Attacks

When attackers gain access to your network, they don't always have full access. With **privilege escalation attacks,** hackers slowly gain access to accounts with higher permissions to access more data. It may take weeks or even months to reach the level they need to view client files. However, it's worth the time and effort for them for them because they can sell the data that they steal online.

Following the Principle of Least Privilege can help to mitigate the risk from these attacks. When fewer accounts can access sensitive information, it becomes harder for hackers to reach that privilege level.

Over time, an account's access level will change depending on what data an employee needs to do their job. For example, does your teller need access to HR documentation? Does HR need to access loan documents? How do you know who has access to what files? Keeping up with these permissions is critical to maintaining the least privilege. A managed service provider can regularly review your accounts to ensure everyone has the precise level of access they need to do their jobs.

▲ **See More at MITRE ATT&CK**

5

Unencrypted Data

It's easy to misjudge the value of information. For example, it might not seem necessary to encrypt a file with a list of client names and addresses. Still, a savvy criminal can piece together small bits of information gathered over time to commit identity fraud and other crimes.

Banks should use strong encryption when sending files, known as a data in transit and storing files, also known as data at rest. Whether the file sits on a desktop or lives in a cloud-based database, if it contains Personally Identifiable Information of business-critical data, it deserves high-level encryption. Luckily, many cloud service providers automatically use excellent encryption to protect organizations.

Make sure you have the right level of protection by having your managed service provider review your current environment and provide ongoing support that ensures you keep data safe.

6

Social Engineering that Targets Employees

Even the highest levels of bank cybersecurity fail when criminals can manipulate your employees. **Social engineering** includes several types of strategies, including:

◄ **Read more at Digital Guardian**

- Phishing techniques that tempt employees to download email attachments or click online links.
- Mimicking otherwise reliable websites and email addresses to trick employees into downloading malware.
- Playing on an employee's emotions to trick them into providing information.
- Posing as authorities that demand access to information.

Shockingly, **nearly all cyberattacks** involve some level of social engineering. Training provides the best protection against social

◄ **See more at ComputerWeekly.com**

engineering attacks. Your employees need to know how to spot signs of fraudulent addresses, resist demands for information, and avoid unsavory websites.

Like a doctor using a vaccination to protect against preventable diseases, using a managed service provider with a fully developed security awareness training and education program can help inoculate your employees against common social engineering attack methods.

7

Internal Attacks

You might not like to admit it, but some cybersecurity attacks come from within organizations. Internal attacks happen often enough that the **U.S. Cybersecurity & Infrastructure Security Agency** maintains a list of protective measures and provides resources to report suspects. What's more, it's not always intentionally malicious insider activity that can pose a threat.

◄ **Read more at the national CISA website**

Someone deleting a critical file by mistake can also cause trouble, especially if you are not prepared with proper backups.

Like most bank cybersecurity threats, a managed service provider offers a proactive way to stop internal attacks before they cause signifcant harm. With 24/7 monitoring, you get alerts as soon as something irregular occurs, and with off-site backups, you can be confident that missing or damaged critical can be quickly restored.

Get the right managed services for your bank by **reaching out to Integris.** Managed IT services focusing on financial institutions makes it possible for our Integris team to provide all the expertise that you need for advanced cybersecurity.

◄ **Find out more today!**

Integris.

Integrisit.com