CAPINTECH

Application Security: Understanding the Risks

By Allison Davis, Senior Manager

Application security is constantly debated. Various regulatory and governing bodies, societies, and institutes have different guidelines for minimum standards, and these recommendations often change as the threat landscape evolves.

How far does your organization truly need to go when implementing application security? And what do you do with these differing recommendations?

Before you can delve into the various controls and determine the sufficiency of your configurations, you must understand common threats affecting organizations and their applications and the impact they can have on your organization.

Common Threats

- **Brute force attacks are rampant.** A brute force attack occurs when a hacker repeatedly attempts to guess your login information. While these attacks had to be conducted manually in the past, now there is sophisticated password-cracking software that tries every possible password combination (e.g., Password1, Password12, Password123). With the enhancements in software and computer processing power, it's only a matter of time before your password is cracked.
- **People consistently practice bad password management**. They use basic dictionary words. They don't change them frequently. They use identifying details, such as the name of their spouse. They write passwords down in unsecured places, like a note on their phone. End users make it extremely easy for a brute force attack to be successful and for passwords to be guessed.
- **Database breaches at other organizations can affect you**. Many people use the same password across multiple systems. A database breach at Facebook may not seem concerning, but what if an employee uses the same password for Facebook and all of your network and financial applications? That can increase the risk of compromise if a hacker obtains an employee's password from Facebook and attempts to access other applications the employee uses.
- **Phishing scams are becoming more sophisticated**. Cybercriminals steal usernames and passwords by sending phishing emails to their potential victims. These emails impersonate legitimate application services with the intent to lure the recipient into clicking on a link that directs him or her to a fraudulent login page. These fraudulent login pages look similar to the legitimate login pages and trick the user into inputting the username and password. The fraudulent page then submits the login credentials to the cybercriminal.
- **Keylogger malware installs on a computer without the user's knowledge.** Cybercriminals also use keylogger malware to obtain usernames and passwords. This malware is installed on the victim's system without his or her knowledge, most commonly when a user visits a malicious website or clicks on a malicious link. The malware captures all the keystrokes the user types, which often include usernames and passwords. The keystrokes are then submitted to the cybercriminal.
- **Default usernames and passwords are often overlooked.** Cybercriminals can access certain systems and administrative portals using default usernames and passwords. This method is more common on hardware devices with web-based administrative portals, such as modems, routers, VoIP, printers, surveillance, and other Internet of Things (IoT) devices. Manufacturers of these products configure a single default username and password for all devices and post this information publicly. Many organizations don't change default usernames and passwords when installing these products on their network, leaving them vulnerable to unintended access.

Impact of Attacks

Hackers have many reasons for attacking, and weak passwords could allow the exploitation of systems, infrastructure, or applications to achieve their goals.

- Some attacks are purely to **wreak havoc**. An attacker who gains access may simply delete data or corrupt systems. Depending on the severity, this could significantly hinder your organization's ability to function.

- Some attacks aim to **disrupt operations**. Some attackers want to prevent an organization from conducting business. Organizations may struggle to recover when this occurs.
- Many attackers aim to **steal sensitive information** they can sell on the dark web or other malicious websites. Depending on the severity, this can have a financial impact due to various breach and privacy laws and regulations. It can also have a reputational impact if your constituents fail to see you as a protector of their information.

Now that you understand the risks, it's important to take steps to reduce them. This article reviews recommended application security settings and outlines steps you can take to enhance your organization's application security controls.

About the Author

Allison Davis, Senior Manager
CapinTech
adavis@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor and senior manager, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinTech

Capin Technology, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA