frogworks

Managing Your Technology So Your Business Doesn't Croak.

2024

Issue 1 Volume 24

Ribb"IT" Review

INSIDE THIS ISSUE:

- What you need to know about business security mistakes
- The importance of Multi-Factor authentication

What You Need To Know About Business Security Mistakes

Data breaches and security vulnerabilities are rising, and not everyone is safe from emerging threats. The NSA and CISA report that many businesses need to follow the best practices. Discover some of the most common business security mistakes and how to stay safe in this helpful guide.

Default Login Credentials Pose the Biggest Threat

Nearly every application or business program executives use has standard default login credentials. Experts recommend only using these factory settings when you first set everything up. As soon as the programs are ready for use, it's best to change the account's credentials. This way, hackers have a lower chance of infiltrating your account. Creating strong passwords for all your accounts is essential to boosting network security, yet reports find that many IT professionals continue to use factory settings.

Harmful Business Security Mistakes

While using default credentials on applications and software is the most prevalent issue, CISA and the NSA note a few other security mistakes businesses regularly make. Experts recommend business owners make correcting these issues a top priority.

Separating User and Admin Privileges

Does your IT department grant anyone access to programs as an admin? Doing so can create big problems if they uncover malicious activity. It's hard to pinpoint where the problem originates if every user has advanced privileges.

Hackers can infiltrate the account and have unauthorized access to important data and information. Therefore, it's critical to only give admin privileges when necessary and give all other users limited access to accounts.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

What You Need To Know About Business Security Mistakes

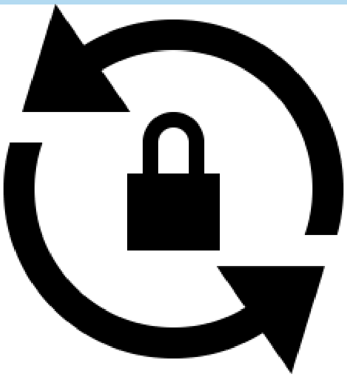
Poor Network Monitoring

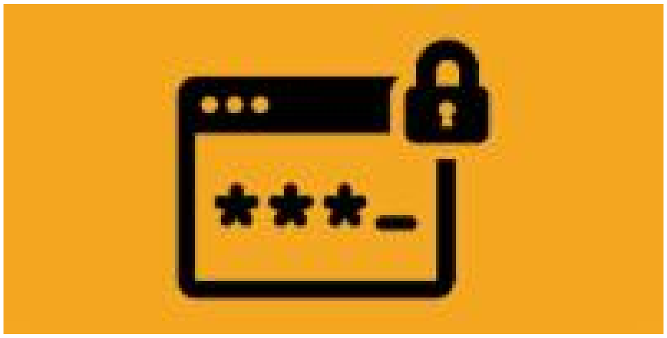
Experts point to a few ways companies need to monitor their networks sufficiently. These include failing to properly set up sensors to collect traffic and end-host logs. Stepping up in this area is essential to improve your business infrastructure and keep your network secure from threats.

Importance of Cybersecurity Measures

Some business leaders don't realize they're dropping the ball on security measures until too late. Falling victim to any cyber attack comes with significant problems, including:

- Loss of integrity and customer trust
- Data breaches
- Financial loss
- Business interruptions





To avoid these costly consequences, technology professionals urge every business owner to emphasize the importance of cybersecurity in their workplace. Making IT staff regularly educate employees on the best practices sets up the entire organization for success.

In addition, it's vital to keep an eye out for emerging threats and take proactive measures. This may include downloading software updates after vulnerability exposure or adjusting security practices at the recommendation of agencies like CISA and the NSA.

The Importance of Multi-Factor Authentication

Business owners and their customers are intimately familiar with trying to log in to some online account before receiving a text message that contains a code. Before you can enter your account, you must submit this unique code, which is a multi-factor authentication mechanism.

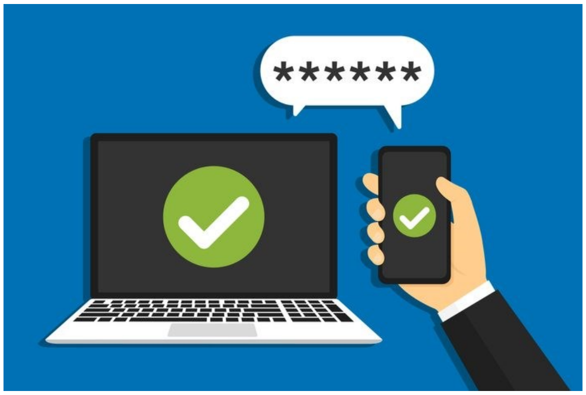
Intuitively, this multi-step security protocol protects sensitive data, including business data and customer information.

Why is Multi-Factor Authentication Important?

Isn't a username and password enough when logging into an online space? No, mainly because data breaches, identity theft, and hacking are more prevalent than ever before.

In many cases, a username and password won't protect your organization's information. The ease with which cybercriminals can figure out a username and password is shocking to most people.

Whether you're a business owner or a casual web surfer, multi-factor authentication is vital to digital security because it requires a user to identify themselves in multiple ways.



How Does Multi-Factor Authentication Work?

Are you trying to access a customer file with sensitive information like a credit card number or an address? With multi-factor authentication in place, the process would look something like this:

- You enter a username and password.
- You receive a message with a four-digit passcode.
- You enter this code after providing the initial username and password.

It's that simple. Of course, you may already know this as a time-based one-time password, which is one type of a multi-factor authentication method. It provides a time-sensitive password for one-time use sent to an email or phone number so that third parties trying to get into your account cannot do so without access to your email or phone.

The Importance of Multi-Factor Authentication

A Word on Adaptive Authentication

Also known as risk-based authentication, adaptive authentication uses several factors to authenticate an attempted login. It covers the following:

- Time: When was the login attempted? Was this during work hours? A login after hours may not be an employee.
- Location: Did the login occur from an unfamiliar location?
- Device: Is this the same device this person always uses?

This additional authentication factor requires the user's identity for verification. That way, only verified users can access your company's data, keeping vulnerable information safe.

A Microsoft report claimed that this kind of multi-factor authentication could block about 99.9% of automated attacks.

Should Your Company Implement More Stringent Authentication Measures?

If you're thinking about the security of your client information or sensitive data, your business is likely in need of a few extra layers of protection. Nearly all industries are at risk of data breaches, though banks and healthcare companies are still among the most frequent targets. Are you ready to face the cyber threats that your business might face online?

Multi-factor authentication through an authenticator app could safeguard your business, keep your organization's data intact, and give you peace of mind about your business's arsenal against cyber threats.

Have a

Great

Year!

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter

Channel Futures
Leading Channel Partners Forward
NEXTGEN 101
MSP TO WATCH • 2021 WINNER