IS YOUR BUSINESS AS SAFE AS YOU THINK?

E-TECH

COULD YOU BE AT RISK?

Hackers know that most smaller organizations are not prepared for network security breaches, making them popular targets for cyberattacks.[1]

[1]15 Small Business Cyber Security Statistics That You Need to Know. thesslstore.com, December 2020

60% think they aren't a likely target of cybercriminals

63% report experiencing a data breach in the past year

23% don't use any endpoint security protections

43% don't have any type of cybersecurity defense plan

47% find data security to be their biggest IT security challenge

74% of SMB data breaches involved external threat actors

YOU HAVE WHAT THEY WANT

Your business is an attractive target because you have items that cybercriminals want, but you may lack the security infrastructure of larger businesses.2

2As Cyberattacks Become More Prevalent, Here's Why Your Small Business is at Risk, securitymagazine.com, February 2020

PERSONAL DATA

Small companies collect data, such as medical records, credit card information, social security numbers, bank account credentials or proprietary business information, that is easy to offload for a profit on the dark web.

CONNECTIONS

A smaller vendor led to the Target breach, which resulted in 40 million stolen credit and debit cards. Hackers accessed the retail giant's system through a subcontractor that provided refrigeration and HVAC systems.

POOR MONITORING

An organization succumbed to a ransomware assault and paid millions for the decoding key to regain their network access. However, they failed to identify how it happened. As a result, they were retargeted by the same group within two weeks.

COLD CASH

Money is a powerful motive, which is why ransomware has become such a popular method of attack. The average cost of a ransomware attack on a business today exceeds $133,000.

FIREWALLS & ANTIVIRUS SOFTWARE AREN'T ENOUGH

Vulnerabilities can be managed only if they have been discovered and identified.[3] Vulnerability scans are typically required quarterly or monthly, depending on the cybersecurity framework being followed.

[3]Costs and Consequences of Gaps in Vulnerability Response study, Ponemon Institute, February 2020

60% were breached due to an unpatched known vulnerability where the patch was not applied

62% claimed they weren't aware of vulnerabilities in their companies prior to a breach

PROTECT YOUR BUSINESS WITH DEFENSE IN DEPTH

Our vulnerability management solution will help you build a firewall and encrypt data both streaming through the network and at rest. Even if hackers get inside your firewall and steal data, it is encrypted.

Contact us today to learn more about how we can improve your IT security.

E-TECH

www.etechcomputing.com
contact@etechcomputing.com
647-361-8191