CHECK POINT™

YOU DESERVE THE BEST SECURITY

TOP 3 CYBER ATTACKS TARGETING SMBs

Today's cyber-landscape is tough for small and medium businesses. Cybercriminals have dramatically improved their attacks, resulting in a higher frequency of attacks and sophistication. SMBs struggle with the expertise, manpower, and IT budget needed to succeed.

Let's have a look at the top three cyber security concerns small business owners face.

#1
Phishing is the leading threat action for SMBs

54%
of SMB attack attempts are successful – resulting in a breach

85%
Ransomware is the biggest malware threat to SMBs

PHISHING

Phishing is a deliberate attempt to obtain sensitive information (e.g. login credentials, credit card numbers, etc.) by masquerading as someone trustworthy. The attack may come in the form of an email that links to a malicious website, or contains malicious attachments.

Other avenues include 'vishing' (voice phishing) and 'smishing' (SMS Phishing)

$17,700
is lost every minute due to a phishing attack [1]

80%
of reported security incidents are Phishing attacks [1]

PASSWORD LOSS

With a stolen network password, it is easy to log into systems posing as that person allowing for movement around the network, infecting other systems, elevating privilege, installing tools as desired, and gathering data throughout.

Using another factor (or 2-factor authentication) can help mitigate breaches from having lost the first factor username and password.

Password dumper was the top malware variety used in reported breaches (most often delivered via Email, usually associated with Phishing, and direct install) [2]

68%
of SMBs worldwide reported that their employees' passwords were lost or stolen in 2019 [3]

RANSOMWARE

Unfortunately, if a small business relies on their computers (as many do for order entry), then a ransomware infection is a show stopper.
At a minimum, there is the threat of losing access to any work or personal files that are not backed up.

1/5 Americans Victim of Ransomware [4]

358%
Malware increase in 2020 [4]

435%
Ransomware increase compared to 2019 [4]

3 steps to understand how ransomware infections occur:

STEP 1 — Gain Access

Consumer-grade equipment like routers and IoT devices have vulnerabilities that are well-known so it's best to do your research before purchasing and installing these. Look for vendors without vulnerabilities and for those who do, see how quickly they can patch the device.

STEP 2 — Data Encryption

After a threat actor has gained access to a system, they can begin encrypting. Since encryption functionality is built into an operating system, this simply involves accessing files, encrypting them with an attacker-controlled key, and replacing the originals with the encrypted versions.

STEP 3 — Ransom Demand

Different ransomware variants issue ransom demands in different ways, but it is not uncommon to have a display background changed to a ransom note or text files placed in each encrypted directory containing the ransom note.

Feel free to download the full white paper here

Find out how to manage your cyber security and learn more here

Sources:
01) https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html
02) https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf
03) https://www.keepersecurity.com/ponemon2019.html
04) https://www.helpnetsecurity.com/2021/02/17/malware-2020/