[COVID-19] Hackers Are Targeting SMBs During the Pandemic & How to Fight Back

Devolutions

SMBS WERE ALREADY VIEWED AS "GROUND ZERO" FOR CYBERCRIME

Before the world became gripped by the coronavirus pandemic, SMBs were already viewed as "ground zero" for cybercrime. Here are some alarming numbers:

- Two-thirds of SMBs have suffered a cyberattack within the last 12 months.
- 80% of SMBs say that malware has evaded their anti-virus software.
- The average cost for an SMB to investigate and clean up after a cyberattack is $690,000.
- SMBs experience 8+ hours of system downtime during a cyberattack.
- One out of every 323 emails received by SMBs is malicious; to put this in perspective, a single worker receives an average of 120 emails per day.

And if you thought that was troubling enough, unfortunately the story has gotten worse. Hackers are taking advantage of the coronavirus pandemic to increase their attacks on SMB remote workers. While all tactics are in play, eight in particular are proving to be especially profitable for hackers and costly for SMBs: phishing, third party attacks, XSS attacks, database hacks, endpoint attacks, ransomware, cryptojacking, and insider attacks carried out by disgruntled former and current employees.

How Your SMB Can Fight Back

The bad news is that there is no 100% guaranteed way to prevent all possible cyberattacks. As long as there are hackers, there will be data breaches. The threat surface is just too vast, and there are too many potential vectors — especially as the business landscape increasingly shifts to remote work (a trend that started well before the coronavirus pandemic but has since accelerated dramatically).

However, the good news is that your SMB can significantly reduce the risk of being victimized by hackers now and into the future. Here are five ways to fight back:

1. Implement Strong Password Policies

Research has found that 74 percent of data breaches start with privileged credential abuse. Strong password management policies include:

- Implementing 2FA/MFA
- Implementing a password manager
- Using passphrases
- Mandating password changes after evidence of a compromise
- Comparing passwords against databases of weak and known compromised passwords
- Enforcing just-in-time access for privileged accounts
- Enforcing a password history policy
- Eliminating password re-use
- Enabling copy/paste passwords (to prevent end users from choosing weaker passwords that are easier to remember and faster to input)

To learn more about these strong password management policies, **please click here**.

2. Train End Users on Cybersecurity

End users have always been — and will always be — the weakest link in the cyber security chain. Here is how the Association of Corporate Treasurers describes this chronic vulnerability:

There are increasingly sophisticated ways of abusing trusted employees and, in today's turbo-charged world, our quest for "cognitive efficiency" makes us particularly vulnerable. Since many business processes still require manual, human input, exploiting this weakest link remains a fertile field for hackers. Our desire to quickly process information with minimal effort has created a unique vulnerability in the digital age. To breach an entire security network, all it takes is a moment for an exhausted or distracted employee to be duped by an email, which may appear perfectly legitimate at first glance, but is really a spear-phishing scam in its most sophisticated form...even the most conscientious employees make mistakes, and hackers know that a single slip-up is all it takes to expose a business to a massive cyber fraud.

To close the gap, businesses need to invest in cybersecurity training so that their end users can be part of the solution, instead of (unintentionally) part of the problem. One of the most effective, accessible and affordable options for SMBs is a cybersecurity training platform, which is an online portal that provides end users with self-paced, hands-on, and skills-based threat detection and mitigation training in a live and dynamic simulated environment. Training can be customized to cover relevant topics such as:

- Social engineering
- Email security
- Mobile device security
- Safe web browsing
- Safe social networking
- Removable data management
- Physical security and environmental controls

Furthermore, supervisors/managers can monitor each end user's progress to identify coaching opportunities. For example, an end user (or a group) may demonstrate sound knowledge of email security but need additional training on mobile device security.

To learn more about cybersecurity training platforms, **please click here**.

3. Implement a Virtual Private Network

Virtual private networks (VPNs) take internet traffic between an endpoint (e.g. computer, laptop, tablet or smartphone) and a server, routing it through an encrypted virtual tunnel. Since hackers don't have the encryption key, they can't snoop and steal the data.

SMBs should install VPN technology on all endpoints in the workplace (or if they prefer, use a Wi-Fi router that has built-in VPN technology). However, the story doesn't end there. SMBs should go a step further and mandate all employees to install VPN technology on any endpoint that they use for work purposes.

To learn more about VPNs, and for a comparison of several popular VPN solutions (updated in May 2020), **please click here**.

4. Ensure That Remote Workers Secure Their Home Wi-Fi Network

Speaking of remote workers: many of them assume that their home Wi-Fi network is safe and secure out of the box. Unfortunately, this assumption is wrong. By default, home Wi-Fi networks are highly insecure, and the only people who are happy about this are hackers.

To secure their home Wi-Fi network, remote workers should do the following:

- Enable network encryption
- Change the default pre-shared key (PSK)
- Change the router's default administrative credentials
- Turn off remote management
- Disable WPS (while this feature is very user-friendly, it is nevertheless a potential security risk)
- Keep the router's firmware updated
- Change the default network name
- Turn off network name broadcasting
- Keep all connected devices secure and updated

To learn more about these important (and 100% free) ways to make a home wireless network more secure, **please click here**.

Also note: some of these recommendations require a little technical acumen, which means that some non-IT end users may be reluctant — or flat out terrified — of implementing them for fear of making a mistake or “breaking” their router. As such, SMBs should provide clear step-by-step instructions, or better yet, use a remote access support tool like Wayk and make the changes for them.

5. Move Data to the Cloud

There are many significant advantages to moving data to the cloud. But for several years “improving security” was not among them. However, this is no longer the case. Today, the cloud is not just as safe as legacy on-premises data centers, but in many cases it’s safer. Here is how Vivek Kundra, Executive Vice President of Emerging Markets at Salesforce, explained this new reality: “Cloud computing is often far more secure than traditional computing, because companies like Google and Amazon can attract and retain cybersecurity personnel of a higher quality than many governmental agencies.”

Here are some additional reasons why data is safer in the cloud than on the ground:

- Cloud service providers monitor security 24/7/365 and conduct ongoing penetration and vulnerability testing, which is a level of continuous scrutiny that many SMBs with limited budgets and smaller IT staff cannot provide.
- Storing data in the cloud helps reduce the frequency and severity of insider threats carried out by negligent and disgruntled employees, contractors and vendors. According to research by the Ponemon Institute, the average annual cost of an insider threat is $8.76 million.
- Unlike on-premises systems that rely primarily on firewall protection to keep hackers out, cloud systems deploy multiple layers of security. Data can also be wiped remotely in the event that machines are stolen or compromised.
- Cloud systems store data in multiple locations, which protects information from hardware failure and corruption. Research shows that recovery times are 4 times faster for SMBs that use cloud services versus those that don’t.
- Most cloud services have built-in security features, such as the ability to shut down any part of a system if a risk or threat is detected, along with app role-based authentication.
- Cloud security is increasingly leveraging AI to find and eliminate threats, and it is using machine learning to automatically get smarter and faster.
- Using cloud apps encourages companies to build a strong, customized threat assessment model to detect potential leaks, and continuously test it (i.e. try and break it) to confirm validity and enhance strength.

To learn more about the security benefits of moving your SMB's data to the cloud, along with best practices, **please click here**.

How Devolutions Can Help

On the business landscape, 99% of organizations are SMBs. Yet despite this, virtually all best-in-class Privileged Access Management, Password Management, and Remote Connection Management solutions are prohibitively expensive and excessively complex for most SMBs — which leaves them vulnerable to security gaps and compliance breaches, reduces their productivity and competitiveness, and risks sending them backward when they need to move forward.

At Devolutions, we believe that neglecting SMBs and treating them like "second class citizens" is wrong. That's why our suite of solutions is:

- Available at affordable price positions and multiple licensing models that make long-term sense for SMBs.
- Highly secured with enterprise-grade protection, logging and monitoring.
- Refreshingly simple and fast to deploy (in the cloud or on-premises).
- Intuitive and easy-to-use for both IT staff and non-technical business users.
- Accessible through smartphone and web apps to support remote working anytime, anywhere.
- Backed by world-class technical support provided by our in-house team of specialists.

Plus, due to the coronavirus pandemic, we have recently introduced some special offers to help SMBs enhance security and productivity during this challenging time:

- The free trial period for Devolutions Password Hub has been extended from 30 days to 90 days — **learn more here**.
- All Wayk Den deployments have been automatically granted an unlimited number of Wayk Now Enterprise subscriptions to connected clients, completely free, until the end of August 2020 — **learn more here**.

Looking Ahead

We have (hopefully) passed the peak of the coronavirus pandemic and are on our way to a healthier future for us all. But when it comes to cybercrime, unfortunately things aren't getting better — they're getting worse for all organizations in general, and SMBs in particular.

We urge you to use the advice and information above to secure your defenses, fight back, and reduce your risk of being victimized by a cyberattack.