Devolutions

The State of CYBERSECURITY in SMBs in 2020-2021

What to Expect in 2021

As we look ahead at 2021, there is some belief that the global coronavirus pandemic will fade, and that fear and dread will finally be replaced by hope and optimism.

However, when it comes to cybersecurity, the situation for SMBs has grown worse in recent months — and things are expected to continue in that direction as 2021 unfolds.

TRENDS ON THE HORIZON + RECOMMENDATIONS

Based our State of Cybersecurity in SMBs in 2020-2021 survey, as well as subsequent developments since the survey report was published, here are four dominant trends that we expect SMBs to face in the year ahead:

1 HACKERS WILL INCREASE THEIR ATTACKS ON SMB REMOTE WORKERS.

Remote working is here to stay. A survey by Gartner found that 82% of business leaders plan to allow their employees to continue working from home after the pandemic (at least part-time, and in some cases full-time). Unfortunately, hackers have noticed this trend as well and have stepped up their attacks on SMB remote workers. The FBI has reported that the number of complaints about cyberattacks to their Cyber Division has risen to more than 4,000 a day, which represents a 400% increase from pre-pandemic levels.

In 2021, we expect hackers to continue their assault on SMB remote workers. While all tactics will be in play, we think eight in particular will be prevalent and widespread: phishing, third party attacks, XSS attacks, database hacks, endpoint attacks, ransomware, cryptojacking, and insider attacks carried out by disgruntled employees (both former and current).

> “To address this threat, SMBs need a Privileged Access Management (PAM) solution that supports critical security features, such as role-based access control, forced strong passwords, Active Directory integration, secure access to privileged credentials, session management and logging, push notifications, automated credential rotation, account brokering, and more.
>
> In addition, SMBs should move data to the cloud, enforce the Principle of Least Privilege (so workers only have access to what they absolutely need for their day-to-day jobs), and ensure that remote workers secure their home Wi-Fi network. SMBs must secure and monitor remote access, in order to keep both remote workers and their organization safe from cyberattacks.”

2 THE MASSIVE CYBERSECURITY SKILLS’ SHORTAGE FOR SMBS WILL GET EVEN WORSE.

In August 2020, the results of a survey by the research and training firm SANS revealed that there is a massive cybersecurity skills shortage, and that the majority of job candidates do not grasp basic cybersecurity concepts, such as common exploitation techniques, computer architectures and virtualization, networking, programming, and data and cryptography. The bad news is that the cybersecurity skills’ shortage is expected to get even worse in 2021 for SMBs, which typically do not have the financial resources to hire a full roster of in-house IT and InfoSec specialists.

To address this threat, SMBs should partner with a Managed Service Provider (MSP) that offers the cybersecurity expertise and resources they need, at a price they can afford. The right MSP is one that: offers a comprehensive range of services, is responsive, provides 24/7 coverage, implements tools and policies to support disaster recovery and business continuity, is technology/vendor neutral, has excellent communication, and is consistent in their efforts.

3 NEGLIGENT EMPLOYEES WILL CONTINUE TO BE THE WEAKEST LINK IN THE SMB CYBERSECURITY CHAIN.

In addition to defending against hackers, SMBs need to protect themselves from an unexpected threat that we expect to continue wreaking havoc in 2021: negligent end users.

These are employees, contractors, and other insiders who through carelessness or incompetence (and often a combination of both) put SMBs at risk by, for example: accidentally sending confidential information to an unauthorized source; failing to heed security warnings about implementing necessary software fixes; and failing to secure laptops, tablets, and smartphones outside the office.

To address this threat, SMBs should enroll their workforce in online cybersecurity training that covers key concepts such as (but not limited to) social engineering, email security, mobile device security, safe web browsing, safe social networking, protection of health information, and more.

While this will not turn them into experts, it will give them the basic education they need to be part of the cybersecurity solution — and not unintentionally part of the problem.

4 MORE SMBS WILL IMPLEMENT A ZERO TRUST NETWORK.

The massive increase in remote workers has triggered challenges for many SMBs related to the use of virtual private networks (VPNs), such as bandwidth bottlenecks that slowdown productivity and frustrate end users, as well as difficulty configuring and maintaining VPNs without in-house expertise. Also, remote workers who use their personal machines and devices can “let down their guard” — and open the door for hackers to breach the corporate network.

To address this treat, SMBs should strongly consider implementing a Zero Trust architecture. The Zero Trust model assumes breach and verifies each request as if it originated from an open (i.e. untrusted) network. Every access request is fully authenticated, authorized, and encrypted, and lateral movement throughout the network is governed by the Principle of Least Privilege (as described above).

When implemented properly, Zero Trust can be an effective defense against sophisticated attacks like the massive Solorigate supply chain attack. Essentially, the motto of Zero Trust is “never trust, always verify.” By removing the assumption of trust and authenticating every action and device, Zero Trust helps SMBs establish a more robust and resilient security posture, while increasing efficiency and productivity.

LOOKING AHEAD

In terms of defending against hackers and preventing accidental data leaks, 2021 will be a very challenging year for SMBs. However, SMBs that adopt the advice provided above, along with the other key recommendations in our State of Cybersecurity in SMBs in 2020-2021 survey report, will significantly increase their ability to prevent and mitigate cyberattacks.

The bottom line? On the cybersecurity landscape, things are only going to get worse for SMBs, and so the time to act is now — not later.