Security Bank

FINANCIALFOCUS

May 2019 | #46-C

CYBERSECURITY : WHAT YOU NEED TO KNOW

Traditionally, large companies and corporations have been the most popular targets for a wide range of cyber threats. However, small businesses are not immune from being targeted and some hackers may even find your small business to be a more desirable target.

This month's article brings some awareness to some of the important statistics.

Best Regards,

Keith Knudsen

KEITH KNUDSEN
PRESIDENT/CEO | SECURITY BANK

7 EYE-OPENING CYBERSECURITY STATISTICS EVERY SMALL BUSINESS NEEDS TO KNOW IN 2019

BY **JOHNATHAN CROWE** | *NINJA RMM*

Businesses don't need to be massive corporations or house treasure troves of sensitive information to be frequent targets of cyber attacks. In fact, recent cybersecurity statistics show that, despite their size, small businesses account for the majority of data breaches (58%).

That's just one of the major key takeaways from several recent industry reports tracking the evolution of cyber crime and online threats. We've gathered additional highlights here for IT pros and managed service providers (MSPs) who need to educate small businesses on the risks they're facing, and who could use some extra ammo for convincing ownership it's not a matter of if they'll face an attack, but when.

Two-thirds of Small and Midsized Businesses have suffered a cyber attack in the past 12 months
So much for the idea that small business = under the radar. Attack campaigns have become so prevalent that if you didn't experience a cyber attack in 2018, you have to count yourself lucky. According to Keeper Security and the Ponemon Institute, you're in the 33% minority. But you can't count on beating the odds two years in a row. Especially when 6 out of 10 small and midsized busiensses (SMBs) also report the attacks they're seeing are becoming more targeted, damaging, and sophisticated.

The average cost of an attack is nearly $3 million
If that number seems high it may be because organizations are thinking of attack costs purely in terms of ransom amounts and neglecting to fully consider the wide-ranging costs of sustained system outages and disruption. In many cases, downtime is the real killer following a breach.

Just imagine the impact of important clients losing access to critical systems, or the sales team being offline with no access to prospecting tools or email. Now imagine that lasting a full work day or longer — according to the 2018 Cisco Cybersecurity Report: Special SMB Edition, 40% of SMBs experienced eight or more hours of downtime due to a breach.

According to the Keeper Security and the Ponemon Institute report, downtime accounts for slightly more than half ($1.56 million) of the $3 million price tag for the average attack.

***Email is the #1 attack vector** - 92.4% of malware is delivered via email*
So how are small businesses being compromised? According to the 2018 Verizon DBIR, the answer is almost always via email.

Attackers see email as a direct line to the most vulnerable part of any network — end users. Why go to all the trouble of utilizing sophisticated exploits and bypasses when you can count on users being human and having a tendency to make hasty clicks?
Malicious emails have come a long way from the easily recognizable spam messages of old, but it's often the simplest messages and disguises that are the most effective.

According to the 2019 Symantec Internet Security Threat Report (ISTR), the most common malicious email disguises are:

1. Bill / invoice (15.7%)
2. Email delivery failure notice (13.3%)
3. Package delivery (2.4%)
4. Legal/law enforcement message (1.1%)
5. Scanned document (0.3%)

In the vast majority of cases (92.2%), malicious emails rely on tricking users into opening attachments. The most popular attachment type by far are Office files, which typically aren't blocked by email filters. According to the ISTR, 48% of malicious email attachments are Office files, up from just 5% in 2017.

Currently, one of the most successful email infection strategies is employed in Emotet and Ursnif campaigns. Once an organization has been infected with one of these trojans, one of the ways they spread is by hijacking victim email accounts and using them to send malicious attachments (often Word docs disguised as invoices) to the victim's contacts. In some cases, malicious emails are even sent as replies to existing email chains, raising the odds of them getting past filters and tricking unsuspecting recipients who recognize the "sender" as someone they know and trust.

Emotet in particular has successfully utilized this and similar tactics on its way to becoming one of today's most dangerous and prolific threats.

84.5% of Q4 2018 ransomware infections were initiated via Remote Desktop Protocol (RDP)

While email is the most popular overall attack vector, when it comes to ransomware, specifically, the vast majority of infections achieve an initial foothold by brute forcing or abusing compromised access to Remote Desktop Protocol (RDP).

RDP is a Microsoft protocol that allows users to connect remotely to other machines. It's commonly used for legitimate administration purposes, but when left exposed to the Internet it draws brute-force attacks like moths to a flame. Once successfully cracked, compromised accounts can be immediately taken advantage of, or sold on dark web marketplaces for a handful of dollars each.

RDP is the go-to gateway for some of today's most active ransomware variants, including Dharma/CrySiS. It's also played a key role in the deployment of Ryuk and SamSam, two variants that have contributed to a dramatic rise in targeted ransomware attacks. In those scenarios, RDP can serve as the initial access point for attackers and/or as a tool to help them achieve lateral movement throughout compromised networks. Before deploying the ransomware, attackers will ensure the stage is set for maximum damage by disabling security software and backups and singling out the victim organization's most critical assets for encryption, specifically.

This approach is becoming increasingly popular — 75% of ransomware infections investigated by security firm Coveware involved wiping or encrypting primary and secondary backups. It's also making infections that much more debilitating and costly to recover from. According to Coveware, ransomware incidents lasted 6 days on average, and cost victims $54,904 in downtime.

4 out of 5 SMBs report malware has evaded their antivirus

What about protecting endpoints with antivirus software (AV)? Unfortunately, reports show a staggering 82% of SMBs have experienced attacks where malware was able to get by their AV. Intrusion detection systems (IDS) don't fair much better, with 72% of SMBs reporting malware slipped past their IDS without being detected.

When choosing endpoint defenses, it's important to select products that aren't relying entirely on signature-matching to detect and block malware.

Patching has become untenable without automation

There were 16,555 CVEs issued in 2018

Email and RDP aren't the only attack vectors small businesses need to worry about, of course. Vulnerable software and out-of-date operating systems can also provide attackers with a way in. Keeping those systems and programs patched is one of those best practices that's easy to say, but far more difficult to do. Updates can be annoying at best, disruptive at worst, and incredibly easy to fall behind on.

Combine that with the fact that there were 16,555 common vulnerabilities and exposures (CVEs) issued last year — 1,529 rated critical — and it's no wonder if a patch or two slips through the cracks. For many small organizations trying to handle patching manually, the goal may not be comprehensive compliance so much as simply picking a few priorities and keeping fingers crossed on the rest.

3 out of 4 SMBs say they don't have sufficient personnel to address IT security

Lacking tools is one thing, but the #1 pain point for small businesses when it comes to securing their network is lack of software or hardware — it's lack of meatware. They simply don't have someone to properly manage security tools and processes in the first place. According to the Ponemon and Keeper Security study, lack of personnel even trumps lack of budget. In some cases, the money is there, and — amazingly — so is the priority. Only 4% of respondents flagged "management does not see cyber attacks as a significant risk" as a top challenge.

The problem is lack of ownership and expertise. Another key finding of the study was that a third of SMBs don't have someone who owns IT security. Nearly half admit they have no understanding of how to protect themselves from today's modern threats.

Conclusion

Statistics can paint a discouraging picture, but the key thing to remember with security is that you don't need to solve everything at once. You just need to focus on making incremental progress one step at a time. Keep in mind any preventative measures you take now will be far cheaper and less time-consuming than dealing with the aftermath of an attack.

The alternative — doing nothing — is easy now, but disastrous in the long run. You can only dodge the bullet for so long. As these statistics show, the risk is only mounting.