Check Point
SOFTWARE TECHNOLOGIES LTD

Quantum
Spark™

THE TOP 3 CYBER ATTACKS TARGETING SMALL BUSINESSES

CYBER THREATS ARE ON THE RISE

No surprise here. Criminals and hackers have stepped up their attacks dramatically over the past year. The United States Federal Bureau of Investigation (FBI) reports that cybercrime has quadrupled during the COVID-19 pandemic. And those attacks are targeting all sectors and sizes of businesses, large and small, but not exactly alike.

54%

of attacks on SMBs are successful - resulting in a breach

The Bad News, the Good News

In an analysis of 3,950 confirmed breaches out of 32,002 security incidents, the 2020 Verizon Data Breach Investigations Report (DBIR) found over a quarter (28%) of all breach victims were Small to Medium Businesses (SMB), i.e. businesses with fewer than 1,000 employees.

While the number for larger enterprises is only

<7%

A bigger concern is that 54% of the attempted attacks on SMBs were successful in breaching their defenses – a success rate nearly eight times higher than that of larger companies. The good news – this is a lower number than in previous DBIR reports.

What it means to an SMB Owner

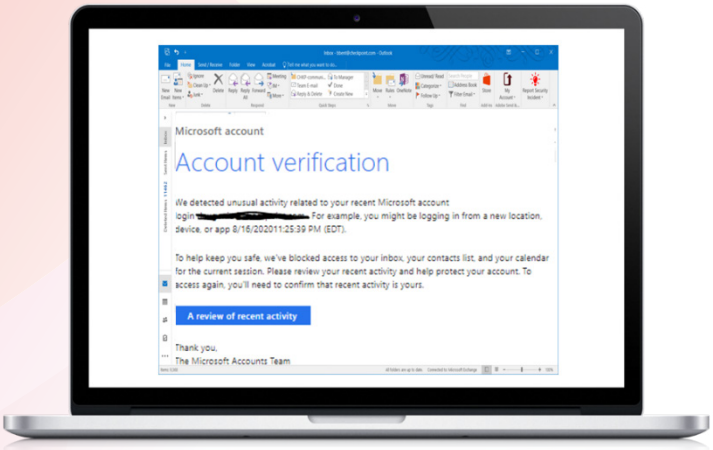
As SMBs have modified their business model to consume more cloud services and web-based tools, attackers have adapted to skim what value they can from their targets. SMB organizations are still a good target for cybercriminals.

There is sufficiently valuable information to make it worth an attacker's time and the organization's protection level is typically weaker than that of a larger enterprise. In the 2020 DBIR, stolen credentials is the data compromised most and threat actors mainly achieve this using phishing techniques. In this paper we discuss the three top cyber security concerns small business owners face; phishing, password loss and ransomware, and cybersecurity measures to prevent them.

ANATOMY OF A PHISH

Put simply, phishing is a deliberate attempt to obtain sensitive information like login credentials or credit card numbers by masquerading as someone trustworthy. The phish may come in the form of an email that links to a malicious website or has a malicious attachment. Other avenues include 'vishing' (voice phishing) and 'smishing' (SMS Phishing).

Some attempts, "spear phishing", are targeted and some are not, "bulk phishing." Spear phishing targets an individual or an organization and may be difficult to detect by appearing to be from a trusted source and having some knowledge familiar to the target. By contrast, bulk phishing casts a wider net, attempting to capture as many pieces of information from different individuals as possible.



A close relative of the phish is the highly targeted attack called a business email compromise (BEC), a scam that can cost companies millions of dollars. This type of attack involves the phisher compromising the account of a high-level executive within a company and instructing their employees to transfer money to an account controlled by the attacker. Even Facebook and Google have taken the bait. See The Top 5 Phishing Scams of all Time.

WHO HAS YOUR PASSWORD?

Having someone's password is akin to having the keys to their car. Like a car theft, with someone's network password, it is easy to log into systems as that person and move around the network, infecting other systems, elevating their privilege, installing other tools as desired and gathering data as they go. Threat actors can essentially impersonate that user.

If only one factor like username and password is needed to login, then they have what they need. There's no need to find a sophisticated zero-day Remote Code Execution bug and a vulnerable system to exploit. This is likely why phishing attacks top the list of attack techniques.

The 2020 DBIR found that password dumper was the top malware variety used in reported breaches and this was most often delivered via Email (usually associated with Phishing) and direct install. This was also reflected in a Ponemon survey where sixty-eight percent of SMBs worldwide reported that their employees' passwords were lost or stolen in 2019. Using another factor or 2 factor authentication can help mitigate breaches from having lost the first factor username and password.

Does everyone have your Password?

Often overlooked, some Internet of Things (IoT) devices like smart cameras and routers come with default usernames and passwords which can easily be found on the Internet. If the vendor doesn't require this be changed when set up, then everyone may have your password. Default and hard coded passwords have been used in botnet campaigns like Mirai and its variants to control hundreds of thousands of IoT devices without their owner's knowledge. Change those default passwords using strong passwords that are hard to guess using brute force techniques.

HELD RANSOM

This leads us to ransomware. 85% of Managed Service Providers (MSP) report ransomware as the biggest malware threat to SMBs. In the 2020 DBIR ransomware is the third most common malware breach variety and the second most common malware incident variety accounting for 27% of the malware incidents.

Unfortunately if a small business relies on their computers and 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. How does a ransomware infection happen?

Step 1: Gain Access - We've seen a few ways this happens. Another notable method is to target vulnerable systems with known exploits. For instance in 2018, the FBI issued a warning about VPNFilter, malware that affected 500,000 small office and home office routers in 54 countries.

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 patched the device. Unfortunately in some cases where a patch wasn't supplied, the recommended solution is to throw away 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. Some ransomware will also take steps to delete backup and shadow copies of files to make recovery without the decryption key more difficult.

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. Typically, these notes demand a set amount of cryptocurrency in exchange for access to the victim's files. If the ransom is paid, the ransomware operator will either provide a copy of the private key used to protect the symmetric encryption key or a copy of the symmetric encryption key itself. This information can be entered into a decryption program (also provided by the cybercriminal) that can use it to reverse the encryption and restore access to the user's files, hopefully.

While these three core steps exist in all ransomware variants, different ransomware can include different implementations or additional steps. For example, ransomware variants like Maze perform files scanning, registry information, and data theft before data encryption, and the WannaCry ransomware scans for other vulnerable devices to infect and encrypt.

PREVENTION IS KEY

Small businesses need enterprise level protection without the complexity, cost and expertise. This means they need security that consolidates the functions to achieve a high level of protection, security that doesn't require a large staff or deep expertise and security that just works, right out of the box. But how does that work?

Above all else preventing the next cyberattack is key. Solutions that detect an infection has occurred are helpful, but they're a bit like hearing "Fire" in a crowded movie theater. When you see or hear the alert, then you know you have to take action, i.e. move quickly to the nearest exit or disconnect the infected system from the network. An alert that the fire is out or the attack was prevented means you can continue doing what you were doing.

SECURING THE NETWORK

Check Point security gateways are enterprise-grade, meaning they've been tested, approved and deployed by thousands of enterprises worldwide. The Check Point Quantum Spark™ Series security gateways are an all-in-one solution for securing small to medium size businesses.

Protection from every threat

Easy to deploy and manage

"All-in-One" solution

Quantum Spark™

- **Easy setup** - Plug it in, follow a simple set-up wizard and your network is secure
- **Out of the box protection** – security policies are included that deliver protection immediately, and adjustments can be made to tailor policies for your business.
- **Low price** - starting at $600, the Quantum Spark family delivers protection with a modest investment. Check Point Quantum Spark security gateways could also be offered by your local Internet service provider as a monthly subscription. Asked for your service provider for Check Point.
- **Easy management** - Ongoing management and upkeep is simple with a mobile app to monitor and mitigate any security issues while on the go.
- **Network and security package in one** – Models are available with Gigabit Ethernet, Wi-Fi and integrated cellular LTE modems. These gateways can support multiple internet service providers and monitor them for quality of service, so you can get the best bandwidth for each application.

Enterprise Capabilities in a Small Package

The security functions of the Quantum Spark Next Generation Firewall family enable you to control who accesses your network, prevents attacks and threats, and secures communications with your business from remote employees or additional business locations. Having the tools is important. Knowing how to use them simply and effectively is critical.

Just like enterprises, small businesses need to ensure that only authorized traffic and users are allowed to access the network. They must also ensure that only appropriate websites are accessed by users. Policies span various capabilities that are used to protect the network.

• Next-Gen Firewall - Ensures only the traffic that should be allowed on the network traverses the network. Prohibited traffic is blocked before it ever enters the network.

• Application Control and URL Filtering - these capabilities work together to ensure that only allowed applications are used on the network and that only allowed websites can be visited.

• User Awareness - Allows an organization to have polices in place that will allow or prohibit what specific people can do, based on their identity or role in the business.

• QoS - Quality of Service allows you to give priority to your most important traffic.

Prevent Attacks and Threats

Large enterprises use high levels of protection to defend the business from threats. Small businesses now can leverage these threat prevention technologies to defend their business.

• IPS - Intrusion Prevention Systems search traffic for attacks targeting business co mputers and devices. Computers and devices that do not have the latest patches are protected by the IPS.

• Anti-Virus - Malware such as viruses and worms are prevalent and can cause major damage. Anti-Virus blocks malware before it can get into the network.

• Anti-Spam - unwanted email is an issue for any business. Anti-Spam blocks SPAM email messages that can also often deliver malware or lead users to malicious sites.

• Anti-Bot - Bots collect information to send to their command and control center for further malicious activity. Anti-Bot will detect and block that communication.

• Sandboxing - prevents infections from undiscovered exploits, zero-day and targeted attacks by launching suspicious files in a virtual sandbox, discovering malicious behavior and then preventing malware from entering the network.

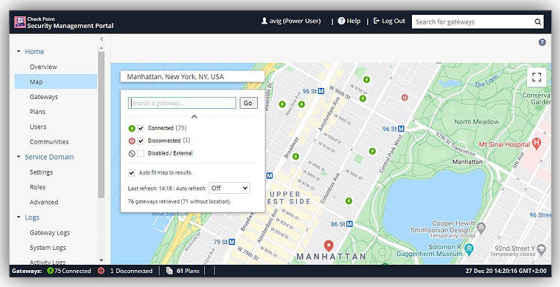
Protect Business Data

When computers communicate with other computers or remote users, the information can be captured by attackers if it is not encrypted. Virtual Private Networks (VPN) encrypts data traversing the network, allowing only the intended receivers to read the information.

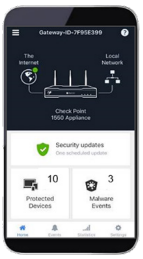
• Remote Access - Encrypts traffic from PC's and user devices to the network, whether they are in the office or on the road.

• Site-to-Site VPN - If a business has multiple offices, this VPN encrypts all communications between multiple office locations.

Cloud Managed Option



Outsourced security services are one of the fastest growing segments in the security market. Security Management Portal (SMP) introduces a central management and service provisioning platform that answers the needs of a Managed Security Provider (MSP) targeting SMBs and vertical markets. It features an intuitive web-based user interface and uses robust architecture to support the management of up to thousands of Check Point 1500, 1600, and 1800 Appliances



Web Browser and Mobile App for Management On-the-Go

SMBs have a variety of easy to use choices for managing Quantum Spark security gateways including a web portal and mobile app. Check Point's WatchTower iOS and Android mobile application enables staff to monitor their security status and quickly mitigate any threats directly from the mobile device.

SECURING THE ENDPOINT

If you don't have a backup plan in place to help you restore systems from a ransomware attack, then consider Check Point SandBlast Agent endpoint security solution.

Ransomware Protection

When an anomaly or malicious behavior is detected, our endpoint security blocks and remediates the full attack chain without leaving malicious traces. Ransomware behaviors such as encrypting files or attempts to compromise OS backups and safely restores ransomware-encrypted files automatically. SandBlast Agent uses a unique vaulted space locally on the machine that is only accessible to Check Point signed processes – in case the malware attempts to perform a shadow copy deletion, the machine will not lose any data.

Phishing Protection

Prevent credential theft with Zero-Phishing® technology that identifies and blocks the use of phishing sites in real-time. Sites are inspected and if found malicious, the user is blocked from entering credentials. Zero-phishing® even protects against previously unknown phishing sites and corporate credential re-use.

SECURING MOBILE DEVICES

SandBlast Mobile is the market-leading Mobile Threat Defense solution. It keeps your business data safe by securing employees' mobile devices across all attack vectors: apps, network and Operating System. Deployment is easy and it protects devices without impacting user experience or privacy.

SECURING CLOUD APPLICATIONS

CloudGuard SaaS is a prevent-first security solution for the protection of cloud email and office applications such as Office 365 and G Suite, Teams, OneDrive, and SharePoint. Connecting to cloud application using native APIs it is invisible to attackers and does not require any network changes.

Once deployed, CloudGuard SaaS scans cloud mailboxes and applications for exiting threats. When a user receives an email, file, or message through an Office 365 or G Suite application, it examines the email for malicious content, and determines if it needs to be quarantined, cleaned, removed, etc. APIs analyze data in transit and at rest to make sure no malicious content penetrates or propagates within the organization, all from a single, user-friendly management platform and a single license for email, office, and enterprise applications.

Business Email Compromise (BEC) Protection

The solution inspects the communication's metadata, attachments, links and language, as well as all historical communications, in order to determine prior trust relations between the sender and receiver, increasing the likelihood of identifying user impersonation or fraudulent messages.

Prevent Account Takeover

Prevent unauthorized users and compromised devices from accessing your cloud email or productivity suite applications. Transparent to users, CloudGuard SaaS provides additional data into the identity provider's authentication process, so suspicious logins (e.g.: seen in two different locations, bad IP reputation) are immediately denied and blocked.

HELP IS AVAILABLE

Nearly two-thirds of small to medium businesses say they lack the in-house skills to deal with cyber-security issues – so it's no surprise that SMBs are urgently looking for solutions to prevent cyber-threats from damaging their business.

Help is available from Managed Security Providers (MSP) who sell security services specifically designed for the growing SMB market. To put the size of that opportunity in perspective, it's forecast that SMBs' spend on security worldwide will almost double between now and 2024 (from around $50 billion currently). And a 2020 survey found that SMBs are willing to pay 25% more to a MSP offering security services, and 91% of SMBs would consider moving to a new IT service provider if it offered the right security solutions.

Why Check Point?

The Fortune 100 relies on Check Point for security. Other providers don't bring the level of expertise and experience delivering high levels of protection. Only Check Point delivers enterprise-grade security in a compact, easy to manage package, designed to meet the needs of a small business.

What Are You Waiting For?

Security for a small business is too important to ignore. With the Check Point Quantum Spark SMB security gateway family, small businesses can feel confident that they have the best security available, in a package that doesn't require extensive expertise or time to get high levels of protection.

Contact a Check Point Authorized Reseller today to get started with enterprise-level security that protects the small business

Visit
https://www.checkpoint.com/products/small-business-security
for more information.

Check Point®
SOFTWARE TECHNOLOGIES LTD