CYBERSTORM

Security Newsletter

21

DEC 21

5 REASONS HACKERS TARGET SMEs

SMEs face significant cybersecurity challenges in this time of increased remote work and the absence of basic security controls.

EASY TARGET 02

The lack of investment in security makes SMEs easy targets for cybercriminals.

SOCIAL ENGINEERING VULNERABLE 04

Lack of basic security expose SMEs to phishing exploits.

UNPREPARED 05

Over 87% of SMEs do not have a plan in place. Another 64% do not have an informal plan of any kind.

06 CONCLUSION

Cyber insurers are scrutinizing payouts by SMEs to cybercriminals. Therefore, SMEs should have a managed security process in place to satisfy insurers when an incident occurs.

THE CYBER EXPERTS
CORE|SECURITY

CORE SECURITY NEWSLETTER

INSIDE THIS ISSUE

SUBSCRIBE TO NEWSLETTER

Please visit our newsletter page and enter your email to subscribe to receive a copy of our newsletter.

CEO MESSAGE

SECURITY IN 2022

I want to take this time to wish everyone a warm welcome to the New Year. Best wishes and success in the coming year from the CORE team. We look forward to working with you again in 2022.

2021 was a very tumultuous year with regards to cybersecurity for many businesses. We were bombarded each day by the news of breach after breach, each more devastating than the last. Due to the scourge of cyber breaches such as Ransomware, many companies lost their customers' and propriety data. In addition, some sustained huge financial impact both by cybercriminals holding their businesses hostage and regulators for non-compliance. In contrast, other companies were forced to close due to the effect of cybercriminals' activities.

Unfortunately, this trend will continue and be even more challenging in 2022. Therefore, we urge you to implement a security strategy to protect your business and prevent cyber breaches.

EASY TARGET

" VICTORIA FAVET PARATO "

The attacks on large firms dominated the headlines. However, small and medium-sized companies are the more frequent targets of cyberattacks. According to the Federation of Small Business, a UK-based group estimates that SMEs suffer an incredible 10,000 attacks per day!

SMEs tend to invest less in cybersecurity than their counterparts, the larger companies, as such they are exposed. A survey by Manta found that 87% of small business owners do not consider themselves at risk of an attack, which sees fewer efforts towards the implementation of security to safeguard their business.

They are also more than likely to have outdated and legacy systems on their infrastructure.

SUSCEPTIBLE TO SOCIAL ENGINEERING

“PREPARATION THROUGH EDUCATION IS LESS COSTLY THAN LEARNING THROUGH TRAGEDY”- Max Mayfield

"Preparation through education is less costly than learning through tragedy.”

Social Engineering is the act of using psychological tricks to manipulate a person into making security mistakes, such as sharing personal information with and wire transfer of money to cybercriminals. At times, even the most well-trained falls victim to these tactics.

Lacking the necessary security process to train personnel, SMEs are a prime target for social engineering attacks such as phishing.

The reason why SMEs are more vulnerable to social engineering is apparent is not just because normal or basic security processes are not in place, but their usage and reliance on certain unmanaged services for their business. For example, controls that would safeguard their business and protect crucial data should be put in place. In addition, SMEs' usage of unsecured cloud services, complete dependency on third parties services, a major source of many breaches, lack of auditing clause in contracts, and the absence of two-factor authentication usage increases the potential of their business being attacked.

RE CONFUSED, IT'S A SIGN YOUR ENEMY IS WINNING."

-Toba Beta

SMEs are lacking in numerous areas of cyber defense, noting that a significant percentage delegate security responsibilities to unqualified IT personnel. It is essential to point out that IT administrators are NOT qualified security resources. They do not have the cyber competence to do the job. Also, segregation plays an essential part in the separation of these roles. These are two very different skill sets and job roles and responsibilities. SMEs' lack of defenses are primarily in the following areas:

- Lack of cyber specialists
- Shadow IT activities
- Absence of security processes
- Protection of customers' data

Several Managed Security Service Providers (MSSP) and IT service providers in today's marketplace are available to work on a contractual or retention basis.

UNPREPARED

" SI VIS PACEM PARA BELLUM"

SMEs are ill-prepared for more significant risks of cyberattacks.

Large corporations have a complex web of protocols and procedures for everything, which also can be said for cybersecurity. But, unfortunately, these procedures are absent when it comes to SMEs.

A survey conducted by the National Cyber Association estimates that approximately 87% of SMEs do not have a plan, while another 69% do not have an informal program in place.

In the absence of a formal process to implement and guide security, employees are likely to underestimate the risks in dealing with security, and security incidents, leaving them vulnerable to social engineering attacks. User security failures are a significant cause of data breaches, access control mishaps, and outright disregard for basic security.

This failure to have a process in place that includes the ongoing educating of employees could be very costly to the companies.

WILLINGNESS TO PAY

READINESS IS KEY

The willingness of SMEs to pay cybercriminals can be summed up to the fact that, 1. They believe there is no other choice, 2. They don’t understand the impact on their business, 3. They don't want it to get out and therefore pay, and, 4. They do not take reputational and trust damages into account. The eagerness to pay for the release of their data further invites attacks against SMEs. The absence of specialists to advise the company, such as a security expert, cyber insurance expert, or lawyer, leave SMEs with no choice but to take matters into their own hands.

The situation surrounding the mindset of SMEs tends to baffle seasoned professionals. First, hiring an IT and cybersecurity specialist on a contractual or retention basis is more cost-effective than the payout to cybercriminals. While these payouts are not as significant compared to larger businesses, they are predictable and provide a steady income stream for criminals.

SMEs should rethink their approach regarding security in 2022 and forward.

CONCLUSION

According to Cyber Claims Report there is an uptick in claims targeting small and midsize businesses, with the frequency of claims increasing by 57% Cyber claims rates are on the rise and the majority of victims are small and medium-sized businesses being hit with cybercrimes like funds transfer fraud and ransomware attacks

The same report indicated that the attacks against SMEs were a suprising increase of 424%! Furthermore, this is made possible by the fact that a majority is working from Home (WFH).

It is imprtant to point out that many cyber-insursers are beginning to scrutinzed claims for Ramsomware payouts more closely, this means not because you have cyber insurance that means your are going to automatically receive a pay-out.

SMEs should consider impleneting a security process that ensure their business are protected by, developing and implementing, an *Awareness program*, *Incident Response*, *Access Control*, *Security Configuration*, and *Vendor Management process*.

CONTRIBUTORS

Contributor (s) to this month newsletter edition.

Cybersecurity Challenges by Wayne. *Wayne Shaw is the Founder and Managing Director of CORE.*

Ethical Hacking and Eagle Eye Firewal Solutions by Babak. *Babak Esmaeili, is the CTO for CORE.*

Newsletter Review and Publication by. Anna. *Dr. Anna Davtyan, is the VP of Sales and Marketing.*

Core is a Managed Security Service Provider (MSSP) dedicated to protecting our clients' business and data, and supporting their people and growth.

The CyberStorm newsletter is a monthly publication by CORE Security.