PiSYS .net

A COMCEN COMPANY

Cyber Security Threats in 2024

We make IT easy

Go back 25 years in business, when digital networks had locks, yet using them wasn't always a top priority. It was more akin to a minor mischief-maker sneaking in rather than a significant threat.

Today, the digital world has undergone a seismic shift. A single lock on your digital door doesn't cut it. What you need are three robust locks, bolted shut, complemented by an alarm system, surveillance cameras, and a formidable security presence.

Businesses of all sizes today are under attack by cyber criminals who use an arsenal of ever-evolving tactics. Gone are the days when digital intruders merely stirred up mischief; now, they wield the potential to cripple operations entirely.

Consider the ransomware onslaughts that have plunged businesses into virtual captivity, rendering them powerless over their own data. Picture the nightmare of stollen confidential business information being sold in the dark web. The aftermath of a successful cyber attack is nothing short of catastrophic, leaving financial ruins and tarnished reputations in its wake.

The landscape of cyber threats is not just expanding; it's morphing rapidly. Staying ahead of the curve in terms of cyber security is no longer an option; it's critical.

As we enter the new year, the question looms: What does 2024 hold on the cyber front? Here's our insight into the imminent threats you should be attuned to.

Let it be known; this guide isn't designed to instill fear but to inform. Understanding the entry points for potential cyber criminals is the first step toward securing your business.

2024 presents its own set of challenges. Be vigilant, stay informed and safeguard.

Cyber Security Threats 2024 that Pose Risk to Your Business

The Threat of New Ransomware

Ransomware is a universal threat that is undergoing a significant transformation. This specialised form of cyber attack involves infiltrating your network, locking you out from accessing critical data and demanding a substantial fee for restoration. The outcomes of a successful ransomware attack are dire, with the potential for irreparable damage.

Cyber criminals are poised to escalate their efforts, utilising advanced techniques in machine learning and artificial intelligence. Brace for a refinement of their extortion strategies, promising increased efficiency and heightened destructiveness. As these malicious criminals set their sights on larger targets, prepare for potential disruptions and financial losses.

Threat Amidst IoT

Familiar with the IoT? It stands for the Internet of Things—devices beyond our computers and phones that connect to the online realm. Your TV, doorbell or even your refrigerator could fall under this category.

Regrettably, these gadgets often boast security measures equivalent to a cardboard fort. Seizing this vulnerability, cyber criminals perceive an enticing opportunity and stand ready to strike.

What's coming is a surge of assaults on IoT devices in the approaching cyber landscape of 2024. Be prepared for potential breaches, where these devices may serve as gateways to infiltrate your network, interlink with other devices to form formidable botnets - where lots of computers are used to attack others. Stay vigilant as the IoT becomes a focal point for cyber threats in the upcoming year.

Unseen Cyber Threats

Advanced Persistent Threats (APTs) are the craftiest assailants aiming for prolonged, unauthorised access to your systems. Their objective is clear—to secretly observe your activities and exploit emerging opportunities.

As we approach 2024, these threats won't merely linger in the shadows; they'll transcend into virtual invisibility. APTs are set to employ sophisticated evasion techniques, including the ominous Living off the Land (LotL) attacks. These deceptive practices involve leveraging your own legitimate software and tools to elegantly bypass your established security controls.

Mobile Vulnerabilities

In 2024, your trusted companions—your mobile devices—are no longer sanctuaries. Cyber criminals are shifting the battleground to your phones and tablets. Prepare for an increase in mobile problems, from malware to banking trojans strategically aiming for your login details. Brace yourself for phishing attacks where cyber criminals manipulate you into using your authentic login data on deceptive sites.

Your mobile gadgets harbour a treasure trove of personal and financial information. Think about the repercussions of a breach, from identity theft and financial fraud to unauthorised access to your most sensitive data. As we step into 2024, safeguarding your mobile devices is paramount.

Under-the-Radar Strikes

Unseen Assaults via Essential Tools: Brace for an upswing in supply chain attacks as we approach 2024. This is where criminals compromise trusted vendors or third-party service providers.

These cyber criminals embed malicious code into seemingly safe software updates or secure privileged access across multiple organisations through these trusted entities. The repercussions of successful supply chain attacks are great — ranging from unauthorised access and data theft to enduring security risks with far-reaching consequences. As we advance into 2024, securing your business against these hidden intrusions is vital.

AI's Impact on Cyber Security

Artificial Intelligence (AI) emerges as The Disruptor, influencing both attackers and defenders. Cyber criminals wield AI to automate attacks, refine evasion strategies and devise sophisticated social engineering ploys aimed at manipulating individuals into specific actions.

On the opposing front, businesses are embracing AI-powered security solutions as a proactive measure to identify threats in real-time. AI takes center stage, assuming pivotal roles in threat intelligence, anomaly detection and incident response. This transformative force is not a fleeting trend; AI is the future of cyber security operations, firmly establishing its presence in 2024 and beyond.

Navigating the Cloudscape: Cloud Realities

When it comes to cloud computing, the sky isn't a limit; it's a gateway to innovation. However, as our reliance on the cloud intensifies, with data accessible across devices and locations, it's crucial to be aware of the distinctive security challenges it brings. This guide dedicates a section to unravel the intricacies of cloud security.

Data Breaches

Misconfigurations, weak access controls and insider threats pose imminent risks, making robust security measures indispensable to prevent potential data breaches.

Insider Threats

While trust in cloud service providers remains high, businesses confront internal risks from employees or insiders. Insider threats may involve deliberate data theft, unauthorised access or inadvertent data exposure.

Shared infrastructure

Operating on shared infrastructure, cloud services introduce vulnerabilities that could grant unauthorised access to resources belonging to other tenants.

Control and visibility

Relinquishing some control to cloud providers is a fundamental aspect, yet it can pose challenges in detecting and responding to security incidents.

Compliance and Regulatory Obligations

Regulated industries must ensure that their cloud deployments align with industry-specific regulations and standards. This encompasses addressing data residency, privacy and data protection obligations, emphasising the critical evaluation of provider compliance capabilities.

Data Loss and Recovery in the Cloud

Cloud outages or disruptions pose risks of data loss or unavailability. To mitigate these risks, robust data backup and recovery strategies are essential, incorporating regular backups, redundant systems and comprehensive disaster recovery plans. Understanding provider backup and recovery mechanisms and aligning SLAs with business needs form the cornerstone of cloud security in 2024.

10 Steps to Fortify Your Defences: Pisys Approach to Cyber Security

At Pisys, safeguarding your business from cyber threats is not just a priority; it's our expertise. Here are 10 proactive steps we recommend to improve your defence mechanisms and ensure the highest levels of protection:

1

Pisys Site Survey Excellence: Before implementing any changes, Pisys advises conducting a comprehensive site survey to assess the current state of your business's security. From our Solutions Specialist carrying out your free survey they can evaluate what you have in place, what you need and provide recommendations and quotes with no obligations. From there we can look at what you want with regards to goals and objectives you want to achieve in the future. We can also answer and solve any problems you might be encountering and we can explain the reasons why.

2

Pisys Prevention Shield: Strengthen your defenses with Pisys's robust security controls. Our approach involves implementing firewalls, intrusion detection and prevention systems, secure network architecture and enforcing strong access controls. Layering these defences creates multiple barriers, significantly reducing the risk of successful cyber assaults.

3

Pisys Detection: Recognising that threats may elude initial defences, Pisys emphasises investing in advanced security monitoring tools, log analysis and threat intelligence. Our approach ensures swift detection, enabling rapid response to mitigate the impact of cyber attacks.

4

Pisys Incident Resilience: Pisys understands that breaches are inevitable. Our well-defined incident response procedures guide your team from containment and investigation to mitigation and recovery, minimising damage and restoring normal operations efficiently.

5

Pisys Vulnerability Reinforcement: Pisys recommends regular vulnerability assessments and penetration testing to identify and patch weaknesses promptly. Our ally in this battle, penetration testing, reveals opportunities by simulating attempts to break into your network.

6

Pisys eCampus: Recognising that your people are both an asset and a potential vulnerability, Pisys advocates for regular cyber security awareness training. Our free programs educate employees on best practices, threats, phishing attacks and the significance of strong passwords.

7

Pisys Data Protection and Encryption: Pisys prioritises data protection through encryption. Even if an attacker gains unauthorised access, encrypted data remains unreadable without decryption keys. Additionally, we assist in establishing data backup strategies and disaster recovery plans to guard against data loss.

8

Pisys Compliance Assurance: Pisys ensures your business meets legal and regulatory requirements related to privacy, data handling and security. Our approach involves implementing specific controls, conducting audits and maintaining documentation to demonstrate compliance.

9

Pisys Continuous Monitoring and Development: Pisys believes great cyber security is an ongoing commitment. Our approach involves continuous monitoring of systems, networks and user activities to detect anomalies and potential breaches. We regularly assess and update security measures based on emerging threats and evolving best practices.

10

Pisys IT Partnership Excellence: Choosing the right IT partner is pivotal, and at Pisys, we recognise its significance. Our team, well-versed in cyber security, collaborates with you to craft the most appropriate protection strategy tailored to your specific business needs. Recognising that a one-size-fits-all approach is rarely effective, we diligently work to create bespoke solutions that prioritise both security and efficiency. Opting for Pisys as your IT partner ensures a seamless integration of all elements, making cyber security a proactive and hassle-free endeavour for your business.

Top Reasons to Choose Pisys for Managed Services:

Accredited Excellence: From ISO 9001, to Cyber Essentials Plus and Green Dragon Certified. Industry-recognised with a strong commitment to social values.

Bespoke Cyber Solutions: Tailored security measures designed to precisely fit your business needs.

Business Continuity: Proven expertise as a Platinum Partner with Datto.

eCampus Training: Free cyber and productivity training for all of your users, ensuring they stay informed and adept in safeguarding your business.

Flexible 30-Day Contracts: Freedom to scale services, 99.5% contract renewal.

Multi-Layered Security Defence: Comprehensive defense against evolving threats.

Remarkable Customer Satisfaction: 99.7% customer satisfaction.

Resource Efficiency: Promoting circular economy, eco-friendly practices.

Seamless Integration Approach: Pisys ensures hassle-free and seamless cyber security.

Top-Tier Security Operations Centre: Vigilant in-house SOC, ready day and night.

We make IT easy

With every year that passes, cyber security becomes increasingly more complex. But when you stay educated about evolving threats, what the dangers are, and stay on top of your security measures with a multi-layered approach, you keep your data and staff better protected.

This is something we help businesses like yours with all the time. If we can help you in 2024,

Get in touch.

CALL: 01792 464748
EMAIL: hello@pisys.net
WEBSITE: www.pisys.net

PiSYS .net
A COMCEN COMPANY