RESTECH SOLUTIONS

WHAT'S LURKING IN YOUR SERVER CLOSET?

CYBER THREATS VS YOUR HUMAN FIREWALL

For some, mistakes breed humility, but for the unfortunate, they're a one-way ticket to misery. Attention to detail is the name of the game, but should you waver, pray the monsters don't come out to play.

Welcome to the life of small and medium-sized businesses (SMBs). On the surface, calm, cool and collected — masters of their domain. Yet, deep down, you know you are just one mistake away from letting cyber monsters have their way with your organization's IT infrastructure. Are you constantly looking over your shoulders thinking, ***"what if I'm next?"***

Unfortunately, it's not a matter of if but when.

Many IT pros and businesses are unaware of the proverbial monsters that aim to attack the weakest aspect of any business's data protection plan – their employees. Or in other words, their "human firewall."

Proactive businesses use everything in their arsenal, from a hodgepodge of business continuity and disaster recovery (BCDR) vendors to expensive security training sessions, to strengthen their organization's security posture. Yet, a careless human error can still cause data loss. This begs the question of what needs to be done to protect IT infrastructures from human fallibility as well as from server monsters that lurk in the dark, waiting for a mistake that gives them the perfect opportunity to strike.

This eBook aims to shed light on the monsters that lurk in your sever closet, luring employees into committing errors, wreaking havoc in your production environment, delaying strategic initiatives and causing major business losses. You'll also learn how to bring an end to their reign of terror, allowing you to concentrate on growth without worry.

RANSOMWARE

Ransomware, in the blink of an eye, can detonate a payload that cripples systems, steals data and destroys businesses.

Cybercriminals are waiting for opportunities to keep ransomware-causing-malware hidden within IT networks for long gestation periods to extract copious amounts of sensitive data, leading to a surge in advanced persistent threats (APT).

APT is a form of cyberattack through which a hacker gains and maintains unauthorized access and remains low key for a significant period. Attackers use the time between infection and remediation to monitor, intercept and turn over sensitive data.

Keep in mind that attackers are finding smart ways to hide malware within IT networks to avoid detection.

HERE ARE SOME PLACES MALWARE LOVES TO LURK IN:

Windows Registry - Malware modifies Windows Registry keys to establish long-term residence within a network and further deploys more malware each time the OS is launched.

Temporary Folders - The loose security surrounding temporary folders makes it a sweet landing spot for ransomware after it enters the system.

.lnk Files - Both malware and ransomware can gain a foothold within a system after propped-up .lnk files, that may resemble an existing shortcut, are downloaded.

ACCOUNT TAKEOVER

Account Takeover (ATO) is used to gain access to user credentials. Cybercriminals, using the dark web, trick users into willingly giving away their logins and passwords before entrapping data across a company's network.

Widespread ATO attacks spring from cybercriminals stealing or buying credentials during third-party breaches and then reusing them to gain easy access to corporate systems to steal IPs, perpetrate business email compromise, gain access to financial accounts and commit other types of cyber fraud.

Remember: A compromised account presents a security loophole that can potentially wreck business reputation and consumer confidence.

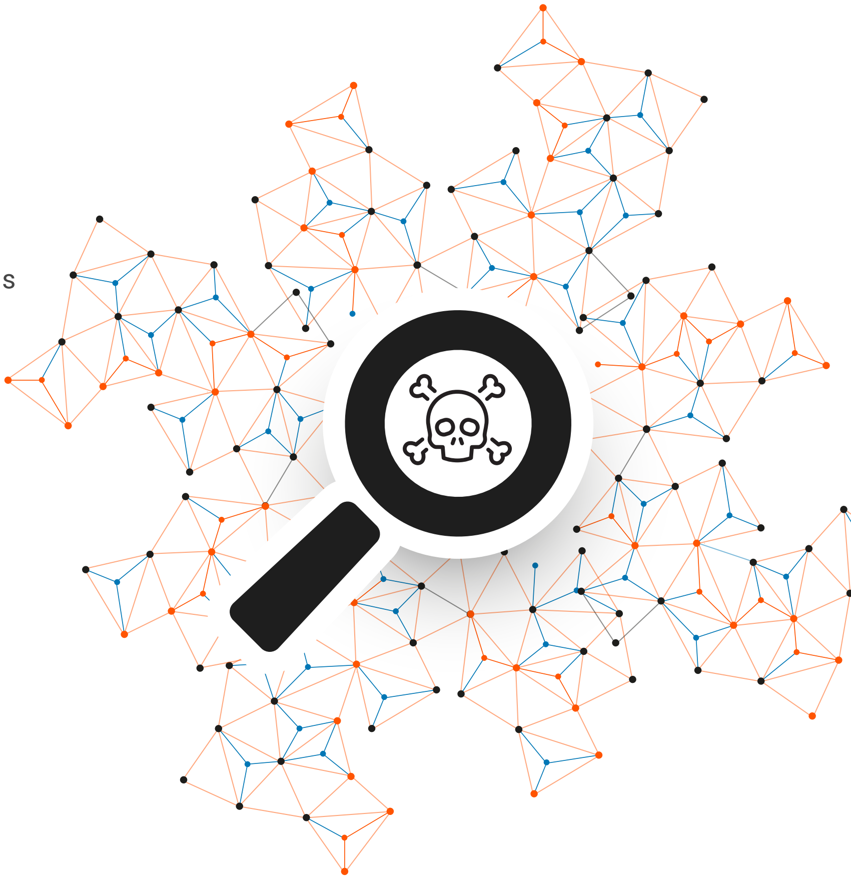
RESTECH SOLUTIONS

PURGE ALL SERVER CLOSET MONSTERS WITH AN EFFECTIVE UNIFIED BCDR

Unified BCDR is your one-stop solution for conquering the cyber monsters that lurk in your server closet and take away your peace of mind. Protect data across physical data centers as well as virtual environments, cloud-native workloads and SaaS applications with ransomware detection, self-healing backups, dark web monitoring and much more.

BE PROACTIVE WITH RANSOMWARE DETECTION

Employ an all-out, multi-pronged approach of endpoint, network, server and backup-level detection to protect data. The predictive analytics engines of BCDR solutions analyze backup data to determine the probability that ransomware malware is operating on a server, workstation or desktop computer. This also includes sleeper ransomware, where victims are unaware of its presence until the ransom demand appears. When ransomware conditions are proactively detected, it's easier to find the source of the threat. If infection is confirmed, you can immediately restore systems from backups tested at the application services level to the last certified recovery point.



TEST TO GUARANTEE FAST RECOVERY

To achieve cyber resilience, regularly test recovery processes to ensure the business is prepared for an actual incident. A Unified BCDR solution with Recovery Assurance performs automatic testing to facilitate an assessment of the viability of the backup – including running trial recoveries up to the point of launching a backup application. This ensures backups are working and ransomware protection is effective. This gives 100% confidence you can meet Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs).

SECURITY INTEGRATIONS THAT ENABLE PROACTIVE DEFENSE AND REDUCE FREQUENCY OF ATTACKS

One of the greatest security investments an organization can make is towards empowering their employees to take part in cyber defense. An effective backup solution for Microsoft 365 provides enterprise-class data protection for Microsoft 365 data, enabling restoration of files, folders, sites and more. Purpose-built security integrations help organizations reduce the frequency and severity of data loss events. Phishing defense empowers IT and security teams to gain actionable insights into threats targeting their organization through investigation of alerts and auto-quarantined emails, the export of real-time threat intelligence to your SEIM solution, and visual cues for employees to alert IT to suspicious emails via automated workflows and feedback loops. Integrated dark web monitoring provides a more complete picture of your organization's security posture with proactive monitoring and alerting of compromised accounts and credentials, which serve as an early warning mechanism before a breach occurs.

Although you've learned about a couple of monsters that target end users by preying on employee behavior, they aren't the only ones out there. Are you ready to tackle them all? You may need a trusted managed service provider to get rid of such nightmares.

RESTECH SOLUTIONS

Although it may seem relatively easy, detecting cyber monsters trying to break into your network is far from simple. That's why it's always best to work with a specialist like us who can make the process as smooth as possible for you. Please do not hesitate to contact us for a consultation.

713-936-6855
info@restech.solutions
https://restech.solutions/contact