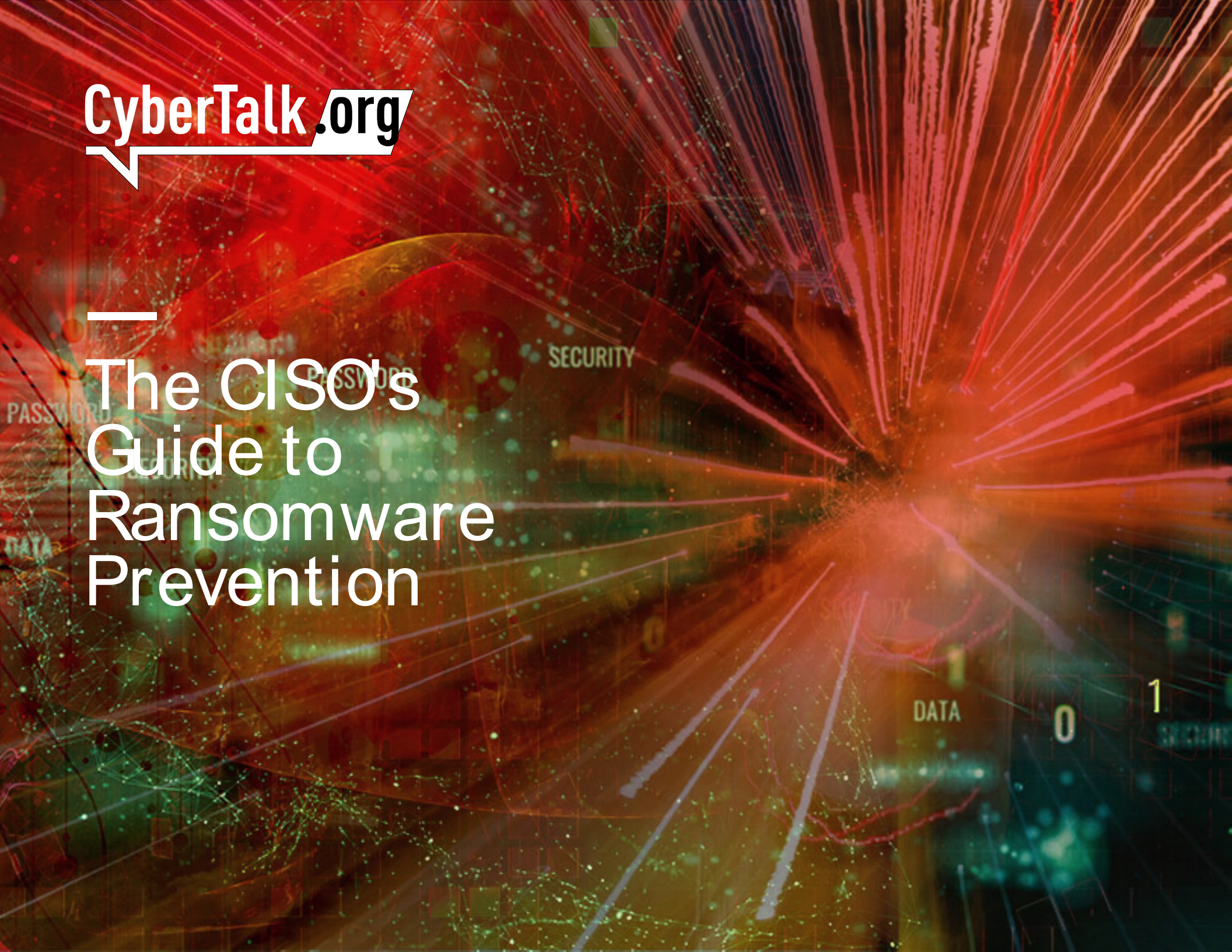
CyberTalk.org
The CISO's Guide to Ransomware Prevention
SECURITY
DATA
0
1

TABLE OF CONTENTS

INTRODUCTION

Ransomware attacks have transformed the cyber attack landscape. These sophisticated and persistent threats can rapidly shut down computers, stop business operations, destabilize economies, and limit access to goods and services in minutes.

Top ransomware attack targets include organizations in the ifnancialservices, healthcare, technology, manufacturing and construction spaces, although many ransomware attackers have proven indiscriminate in choice of targets.

Cyber crime gangs probe vulnerabilities within an organization, determine how to create chaos, and disruption, and then plan for proifteering.Some hackers opt for a "smash n' grab" approach, while others lurk quietly in systems for months in order to maximize levels of disruption and ifnancialgain.

The average ransomware attack costs business around $3.86 million.[1] Exceptional cases, such as the WannaCry ransomware worm, have led to outstanding expenses. WannaCry is estimated to have caused $4 billion worth of damage, worldwide.[2]

WannaCry has caused an estimated US$4 billion worth of damage, worldwide.

While the total cost of ransomware and ransoms continue to trend upwards, ransomware attacks need not be a routine business expense or included in the cost of operating a business.

With higher levels of cyber security maturity, organizations can develop more resilient environments.

---

[1] Cost of a Data Breach Report 2021, IBM

[2] Ransomware: A Constant Threat, Kirk Hayes, Infosecurity Magazine, Feb 21, 2022

RECENT RANSOMWARE EVENTS

Financial Services

Earlier this year, a multi-trillion dollar South Africa-based investment administration provider experienced a ransomware attack. The investment group remained unable to access systems for ifve consecutive days. Although the group's ifnancial assets were not at risk, the outage reduced clients' abilities to process investment-related instructions and restricted other services.

Amidst the outage, the affected ifrm was unable to update prices for certain brokerage portfolios.

90% of financial institutions are believed to have been hit with ransomware.[3]

The investment group is among a large number of private and public sector ifnancial entities that have fallen victim to ransomware. The banking sector has witnessed a disproportionate number of attacks; experiencing a 1,318% year-over-year increase during the ifrst portion of 2021.[3]

Healthcare

Healthcare organizations are another favorite among ransomware attackers. Across the past few years, medical groups in the US, Australia, and elsewhere have contended with devastating ransomware attacks. Attacks have led to the compromise of patient data; from social security numbers, to personal health record information.

At least one medical organization decided to permanently close its doors after failing to recover ransomed data. As the cyber risk to the healthcare sector expands on account of the geopolitical climate, efforts to protect hospitals, health clinics, employees and patients must increase.

Why financial services and healthcare organizations? Millions of dollars in the bank and/or valuable data = high profits.

---

3 Banking Industry Sees 1381% Increase in Ransomware Attacks in 2021, Maria Henriquez, Security, September 20, 2021

DYNAMIC TRENDS

Ransomware-as-a-Service

Historically, ransomware attacks were largely conducted by ransomware gangs. A ransomware operation was a dififcult feat to pull off alone. However, new Ransomware-as-a-Service software enables any threat actor to invest in "off-the-shelf" ransomware products. In turn, any individual can independently execute a ransomware attack.

After Ransomware-as-a-Service (RaaS) based attack is launched, the threat actor's victim or victims are directed to the RaaS operators' payment portal. In some cases, the operators provide "customer service" to help victims pay extortion fees.

Triple extortion threats

Free online ransomware decryption tools, data backups and other savvy tactics can help victims circumvent the dififculties caused by ransomware attacks.

For example, enterprises can contend with encrypted ifles by restoring data from backups, making ransom extortion payment obsolete.

Hackers have caught on. New ways of bringing organizations back to the negotiating table are emerging. Chief among them? Threatening to leak sensitive data belonging to clients or threatening a Distributed Denial of Service attack against the target organization.

These days, ransomware not only means infrastructure disruption and a potential for leaked internal data; ransomware threats are now very multi-dimensional.

The bottom line is that ransomware threat actors are adding additional layers of pressure in attempts to force organizations to part with their resources.

Common Ransomware-as-a-Service Strains

- **Ryuk ransomware.** Experts estimate that Ryuk results in about one third of ransomware infections.
- **LockBit ransomware.** LockBit has existed for several years, but has recently become a part of RaaS operations.
- **REvil / Sodinokibi**. This type of ransomware has affected major organizations worldwide.
- **Egregor / Maze ransomware.** Although Maze has stopped its operations, related ransomware variants – like Egregor - remain operational under the RaaS affiliate model.

The Ransomware-as-a-Service strains mentioned above represent a fraction of the number of ransomware strains that exist. However, these have had significant impact on businesses and as a result, RaaS "affiliates" find them lucrative to deploy.

RANSOMWARE, MSPs, AND MSSPs

In July of 2021, a ransomware attack hit the IT ifrm known as Kaseya. The attack's aftershocks were felt by all of Kaseya's clients, and their client's clients. This could occur because the aforementioned ifrm is a managed service provider (MSP), meaning that they distribute computing services to other organizations. In turn, these organizations provide computing services to even smaller businesses.

The Ransomware-as-a-Service afifliate who conducted the attack clearly intended to propagate the ransomware to Kaseya's MSP customers. Once the ransomware attack blighted Kaseya, it also immediately affected at least 1,000 additional enterprises. A $70 million ransom payment (in Bitcoin) was requested in order to compensate for all organizations' victimization.[4]

As the aforementioned example shows, MSPs and MSSPs may be at elevated risk of ransomware attacks. They represent easy conduits for attacks, with a potential for downstream effects and corresponding increases in proifts.

Experts contend that MSPs and MSSPs often fail to take the threat of ransomware seriously. Those that retain sophisticated, strong cyber security infrastructure may be able to weather the storm.

Actionable cyber security steps for MSPs and MSSPs:

- Conduct a risk assessment
- Initiate vulnerability scanning
- Identify a strong cyber security partner (vendor)
- Invest in cyber security solutions that address all attack vectors; email, endpoint, mobile, and more
- Develop and regularly update a cyber incident response plan
- Follow best practices around cyber security; patching, timely software updates, education awareness programs, etc.

Given the increased incidence of ransomware attacks on service providers, organizations should take the opportunity to pursue stronger security.

---

4 Kaseya, what this ransomware attack fallout means, Cyber Talk
https://www.cybertalk.org/2021/07/06/kaseya-what-this-ransomware-attack-fallout-means/

PREVENTION

To prevent ransomware attack damage, implement these cyber hygiene habits and best practices:

1. Provide employees with cyber security awareness training. Many ransomware attacks start with a convincing phishing email sent to an employees' inbox.
2. Develop stronger user authentication methodologies; these include multi-factor authentication and password policies.
3. Ensure that your organization retains usable backups of all critical data, databases, key applications, and servers in non-networked locations.
4. Test backups regularly as part of your ransomware prevention strategy.
5. Segment networks to prevent lateral movement in the event of a breach.
6. Regularly update and patch software. Organizations have needlessly suffered security incidents due to patching oversights.
7. Deploy proven, effective threat detection tools. Opt for automated threat detection, which can increase advanced attack identiifcation capabilities.
8. Filter most threats out of systems before they can cause harm by using automated email security and endpoint security tools.
9. Pursue a 'defense-in-depth' approach, which refers to layering security measures.
10. Stay up-to-date regarding the latest security threats through vendor-sponsored blogs, like CyberTalk.org.

EXPERT INTERVIEW HIGHLIGHT

Giorgio Brembati, Cloud Security Architect and Office of the CTO

The prospect of a ransomware threat can feel daunting. For some, ifghting ransomware may even feel hopeless. Here's what one of Check Point Software's experts has to say on that front…

In a Cloud Security Architect role, Giorgio Brembati works within the Check Point Software EMEA team of specialists for southern Europe. He supports customers and companies in adopting strategies, architectures and solutions to secure their environments in public and private cloud contexts.

How has ransomware affected cloud computing infrastructure?

Most organizations today rely on the cloud, and over the last few years, we have seen it become one of the crucial components of IT organizations. We have seen companies moving virtual desktop infrastructure (VDI) environments and virtual machines (in a lift/shift approach) and then start utilizing native services.

When we take a look at the protection that is put in place along with this first migration technique, we can see how native systems do not provide threat prevention capabilities. Companies should rely on anti-malware and emulation techniques to prevent known and unknown attacks that may reach IaaS systems from both trafic and workload perspectives.

In what ways are cloud technologies uniquely vulnerable to ransomware?

In cloud environments, we frequently see the extensive usage of Platform-as-a-Service services with databases and storage. In a context defined by a shared responsibility model that represents a customer as responsible for the data, the correct configuration of these services becomes crucial to implementing proper security practices. These services are based on extensive flexibility and availability, and bring up the question of how to control the exposition and settings in our storage or database provided as service. If we then expand our view to how companies use cloud environments today, we can identify a trend that focuses on multi-cloud environments, making these security practices even harder without multi-cloud security solutions.

DEFENSE

In the event that a ransomware attack hits your organization, here's how to respond:

1. Contain the breach. Mitigate damage efifciently and avoid allowing the attack to worsen.
2. If possible isolate the infected device/s from your network
3. Ensure that all traces of the ransomware/malware are removed from your system.
4. Scan backups to check for malware. If no threats are found, attempt to restore data from backups.
5. Contact internal IT administrators and executives who should know about the attack.
6. Organizations are also encouraged to reach out to law enforcement, as appropriate.
7. Avoid paying ransom extortion fees. Decryption tools are not guaranteed to work and hackers can still choose to leak data.
8. Regardless of whether or not you maintain a cyber insurance policy, contact your business insurance group.
9. Appropriate departments to notify clients other business relations who may have been negatively affected by the breach.
10. Reach out to your cyber security vendor, which may be able to offer further insights into your speciifc ransomware experience.

CASE STUDY: Medical Advisory and Outread (MOA)

Stopping next generation ransomware threats

When a new Division Manager of IT joined Medical Advisory and Outreach (MAO), he realized that the organization's current infrastructure could not support the organization's new needs. The group needed to upgrade security, scale security to meet new needs, adhere to speciifc compliance requirements and stop malware/ransomware threats.

Solutions: Above and Beyond

To secure clinics as quickly as possible, the new Division Manager deployed Check Point Security Appliances. This immediately gave cyber security specialists at-a-glace visibility into system' compliance status, improved efifciency, enhanced privacy of client data, and prevented both malware and ransomware infections.

When ransomware attacked a user's browser, Check Point stopped it instantly, preventing it from encrypting MAO ifleshares.

Solutions: Above and Beyond

Check Point gives me and my teams' full conifdence in our ability to grow and effectively maintain security and privacy," said the Division Manager. "I've worked with most of the other products out there, and Check Point gives me the most peace of mind."

SOLUTIONS

Specific solution types that can help…

1. Prevention-focused solutions that leverage AI within a multi-layered security architecture are best.
2. An intelligent, consolidated ransomware prevention architecture can prevent known and zero-day attacks.
3. Consider purchasing anti-ransomware tools that are part of a larger cyber security solutions package.
4. Seek out cyber security solutions that offer a high ROI and low TCO.

IN CONCLUSION:

Ransomware threats can easily undermine enterprises. The threat persists across industries and across geographic locales. Roughly hewn cyber security architectures are not tough enough to combat next generation threats. The best approach to fighting off ransomware starts with prevention. While there are never any guarantees, with a strategic cyber security roadmap, it is possible to win the fight. For further expert insights into the ever-changing ransomware threat landscape, visit Cyber Talk.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com
U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233
www.checkpoint.com