CyberTalk.org

The CISO's Guide to Ransomware Prevention

TABLE OF CONTENTS

INTRODUCTION

Ransomware attacks are devastating businesses by knocking down systems and blowing up budgets. These sophisticated and persistent threats can disrupt computer functions, grind business operations to a halt, limit access to services, reduce the production of goods, and result in significant monetary losses. Top ransomware attack targets include firms in the financial services sector, the healthcare sector and the construction industry, although many attackers don't discriminate in terms of where to look for a potential goldmine.

In the last five years, ransomware attacks have increased by 13%.[1] If that sounds inconsequential, in the first half of 2022, experts observed roughly 236.7 million ransomware attacks. The average cost exceeds $1.8 million per incident, and costs are expected to balloon to $265 billion by 2031.[2] The numbers don't even tell the entire story. More ransomware attacks occur than are reported, meaning that a greater quantity of private information is likely compromised than known and that projected total costs may reflect an underestimate.

Businesses fall victim to ransomware attacks everyday. Many organizations have resigned themselves to the notion that they will, at some point, weather a ransomware event. However, ransomware is preventable. It should not be accepted as a facet of the new normal and here's why:

In exchange for restoration of systems and/or data, ransomware groups always demand a ransom. Yet, the payments typically finance a vicious cycle of continued ransomware development and deployment, hurting other enterprises and the larger business ecosystem. In some cases, ransom payments have been known to finance illegal or immoral activities; from intellectual property theft to terrorism.

With higher levels of cyber security maturity, organizations can develop more resilient environments. Will your organization emerge victorious in the battle against ransomware threats? In this eBook, see the challenges in a new light, and discover how to navigate them so that you can execute on strategic objectives, meet security goals, and prevent negative business outcomes.

---

[1] Top Insights from the Most Notorious Ransomware Attacks and Attackers, CyberTalk.org, March 10, 2023

[2] Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031, David Braue, Cybercrime Magazine, June 2, 2022

RECENT RANSOMWARE EVENTS

Financial Services

In January of 2023, ION Cleared Derivatives, a division of ION Markets, experienced a ransomware attack that impacted some of its derivatives services. Systems were temporarily offline and financial institutions were forced to manually confirm trades.

Issues with data submissions meant that large trading companies were advised to estimate commodity prices and to revise them later in an effort to avoid extended reporting delays.

The U.S. Commodity Futures Trading Commission, a regulator, waited to publish weekly trading statistics because some affected ION customers were unable to collate information fast enough to create daily positioning reports.

A market player with insider knowledge of the situation conveyed that thousands of firms could have been affected by the attack.

According to Reuters, two negatively impacted firms likely included ABN Amro Clearing and one of Italy's banks.[3]

Healthcare

In March of 2023, the Hospital Clinic de Barcelona, in Spain, fell victim to a ransomware attack. In turn, the hospital was forced to cancel thousands of medical appointments, and had to shut down laboratories, clinics and the emergency room.

In numbers, 3,000 patient checkups, including radiotherapy visits, and 150 non-urgent operations were canceled in the immediate aftermath of the attack.

Said the telecommunications secretary for the regional Catalonia government, Segi Marcen, "We will not pay a cent," expanding his comments to note that the hospital would not pay a ransom demand if one were demanded.

Hospital staff were temporarily forced to use paper and pencil, and did not have access to electronic patient data-sharing systems. Urgent cases were diverted to other hospitals.[4]

---

[3] ION Brings Clients Back Online After Ransomware Attack, Harry Robertson, Reuters, February 7, 2023
[4] Ransomware Attack Spreads Chaos at a Hospital in Barcelona, Paulina Okunyte, Cybernews, March 10, 2023

DYNAMIC TRENDS

Ransomware-as-a-Service

Historically, ransomware attacks were largely conducted by ransomware gangs. A ransomware operation was a difficult 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 difficulties caused by ransomware attacks.

For example, enterprises can contend with encrypted files 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.
- **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 firm 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 firm 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 affiliate 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 profits.

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 identification 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

Jeff Schwartz | VP Security Engineering, North America, Check Point

The prospect of a ransomware attack can be daunting and misperceptions in relation to ransomware can muddle situations. Here's what Check Point's Jeff Schwartz has to say on that front...

Jeff Schwartz is the VP of Engineering, North America, for global cyber security company, Check Point Software. He manages a team of 200~ engineers across multi-disciplinary fields, and he's responsible for all security engineering resources across a $1 billion portion of the business in North America.

Over his 20-year career in cyber security, Jeff has consulted, designed, and overseen the implementation of the largest network security deployments across all industries, and throughout both the Fortune 500 and major government agencies.

Tell us about common misperceptions that you're seeing in relation to ransomware?

The biggest misperception is that good enough security is good enough. While it's true that some security is certainly better than nothing, there are two issues with this. One is that most endpoint solutions don't provide thorough preventative and recovery capabilities when it comes to ransomware. And secondly, we're seeing vast increases in ransomware across IoT and the internet of medical things, which are generally unsecured from ransomware.

How can security professionals catch a ransomware attack before it starts?

This is why better prevention is critical. Most organizations have relatively flat networks internally. This is an important factor in why attacks can so freely move across a network from one area to another. There are two characteristics of providing better preemptive enforcement (or prevention):

1. Many diverse engines are needed to provide inspection across mobile, endpoint, workload, cloud and network.
2. Better threat intelligence so those engines can provide thorough, accurate prevention without impacting "business as usual" traffic.

DEFENSE

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

1. Contain the breach. Mitigate damage efficiently 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 specific 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 specific 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 efficiency, 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 fileshares.

Solutions: Above and Beyond

Check Point gives me and my teams' full confidence 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 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com