ENTERPROTECT

WHITE PAPER

Ransomware Prevention for IT Pros

Best Practices for Keeping Your Company Secure

WWW.ENTERPROTECT.COM

Disclaimer

Nothing contained in this document or relayed verbally will be deemed to amend, modify or supersede the Enterprotect Terms of Service or any other terms and conditions of any written agreement between the reader or reader's company and Enterprotect, or Enterprotect's subsidiaries or affiliates. Enterprotect does not make any promises or guarantees that any of the methods or suggestions described in this document will provide 100% protection against cybercrime, cyberattacks, disaster or similar incident. This document is not intended as legal advice nor should you consider it as such. The reader exclusively assumes all risk of utilizing or not utilizing any guidance described in this document.

ENTERPROTECT

Introduction

Ransomware is a type of malicious software that is used to extort money from individuals or businesses by blocking access to their data. It works by encrypting files on the victim's computer, making them inaccessible until the ransom is paid. The cybercriminal groups responsible for ransomware attacks are becoming increasingly sophisticated in their tactics and more aggressive in their targeting of victims. Businesses are particularly vulnerable due to the amount of sensitive data they store, making them attractive targets for attackers.

Ransomware on the Rise

Ransomware attacks have been on the rise in recent years, with a notable increase in the frequency and severity of incidents. In 2022 the World Economic Forum (WEF) reported that there had been a 255% annual increase in reports of cyber-attacks worldwide, while security firm Emsisoft reported that there were over 587 million successful ransomware attacks in 2022. Experts expect ransomware growth to continue unabated in 2023.

The cost of ransomware attacks is also expected to rise substantially in the coming years. According to a new report, the average cost of a ransomware attack in 2022 was more than double what it was in 2018. According to Coveware, the average ransom payment in 2022 was $228,125, while the median ransom payment was $36,360, and the cost to recover from a ransomware attack ranged from 5x-20x the ransom payment. According to the same study, 71.9% of businesses affected by ransomware had between 11 and 1000 employees, and they experienced an average of 24 days of downtime.

Due to the increasing threat ransomware poses to every organization, it's no wonder Ransomware is a top concern for IT professionals and management alike.

Best Practices to Prevent Ransomware Attacks

Keep Computers Up-to-date

IT professionals should keep their computers patched to protect against ransomware. Keeping computers patched is an effective way to prevent some ransomware variants from compromising a computer, as patching fixes security vulnerabilities that ransomware exploits to infect the system.

Educate Your Users

Email is now the #1 method of infection for ransomware, with more than 54% of reported infections resulting from emails containing malicious attachments or links. IT professionals should ensure that all employees are educated on the risks of ransomware, such as not clicking suspicious links or downloading unknown files. By implementing these measures, businesses can better defend and prevent ransomware attacks.

Implement Vulnerability Scanning / Management

Virtually every device and application has known vulnerabilities. While many organizations are good at keeping their firewalls and operating systems up-to-date, many don't have the tools needed to detect vulnerabilities in other devices and software. Ransomware developers routinely use these, often unpatched, vulnerabilities to initiate a ransomware infection.

By implementing an effective vulnerability management process, organizations can identify weaknesses in their systems before they are exploited by ransomware or hackers. Vulnerability Management includes regularly scanning systems and networks for vulnerabilities and patching them as soon as possible.

Segment and Restrict Access to Certain Data and Networks

Lateral movement is the #2 method of infection for ransomware. Lateral movement is the process of moving throughout a network once an initial breach has occurred. Ransomware variants that use this technique are extremely dangerous because the ransomware can spread quickly and infect data across entire networks. This method is also used to

locate and encrypt backups stored on network shares, on file servers, and Network Attached Storage (NAS) devices.

IT professionals should consider segmenting their networks, firewalling traffic between those networks, and restricting access/communications to only those users/devices that need it.

Harden Your Systems

There are a number of free resources (including those published by Enterprotect https://www.enterprotect.com/resources/) on the topic of system hardening. Hardening is the practice of implementing settings that secure a system beyond the system's default configuration.

Implement a DNS Security System

One major way ransomware spreads is through malicious URLs. These URLs can be shared in emails, SMS text messages, on chat forums like Discord or Slack, and even in advertising campaigns on reputable websites.

These websites can host drive-by-downloads, where just visiting a site force-downloads malicious software onto your computer that will initiate a ransomware attack. Phishing campaigns and social engineering are also responsible for spreading ransomware. Fake social media accounts or too-good-to-be-true deals will often point users to malicious URLs, forcing malware downloads.

One of the best ways to combat a ransomware attack is to block threats at the DNS layer. DNS security not only blocks domains hosting ransomware but will also stop “callbacks” from malware to "command and control" servers. This can prevent ransomware from obtaining the encryption key necessary to encrypt the computer.

Invest in Effective Protection

Many IT professionals assume that antivirus software easily detects and stops ransomware. While that may prove true for some variants, the unfortunate fact is that antivirus does not provide adequate protection against most ransomware. Antivirus software works by scanning for known threats based on an ever-evolving list of identified viruses. However, these lists cannot keep up with new ransomware variants as they're constantly changing and evolving to evade detection from traditional security measures like antivirus programs. As a result, even if you have the most up-to-date version of an antivirus system, it may still not be enough to protect you from ransomware attacks.

With ransomware, the stakes are too high to rely on technology that's ineffective against the latest threats. Organizations need to make the change to behavioral detection systems that analyze how files and executables behave rather than how they look.

Prepare for a Ransomware Attack

It's becoming increasingly difficult to avoid ransomware attacks as the number of cyberattacks, and malicious actors continues to rise. Statistically, falling victim to ransomware is less of an "if" and more of a "when". As such, IT professionals need to work with their executive team to prepare for a ransomware attack. By preparing, IT teams can help limit the damage caused by an attack and ensure their organization can recover quickly.

Implement 24/7/365 Security Monitoring

The speed at which your organization can respond to and isolate cyberattacks such as ransomware can dramatically impact the extent of the damage caused by such an attack. Waiting hours or days to respond to a cyberattack can allow the threat to spread, increasing downtime and causing recovery costs to climb exponentially.

Implementing a 24/7/365 Security Operations Center staffed with experienced cybersecurity professionals, armed with the latest security tools isn't a cost-viable option for most businesses. Organizations should consider outsourcing their security monitoring.

Fortify Your Backups

Backing up critical data is essential for businesses to guard against ransomware attacks. Paying the ransom can be costly, doesn't always guarantee you get your data back, and encourages attackers to continue their operations, perpetuating the growth of ransomware. IT professionals must work to fortify their backups to ensure they can recover their organization's data without paying the ransom demanded by hackers.

Having multiple backups of important files can help organizations prepare for and prevent ransomware attacks. Regularly backing up data on both local and cloud-based services provides an additional layer of protection in case of a ransomware attack or other system failure. Companies should also consider offline storage options to ensure that backups remain safe from attack even if the backup system is compromised.

Invest in Cyber Insurance

Investing in cyber insurance coverage is an important decision for organizations of all sizes. Cyber insurance can protect from the financial losses that may occur if a company experiences a data breach or a ransomware attack. Cyber insurance policies can cover the costs associated with recovering from such an attack, including the ransom itself, legal fees, and other damages incurred. It is essential for any business that handles sensitive data to have robust cyber security measures in place, and investing in cyber insurance coverage provides additional peace of mind that your business will remain secure and protected against potential threats.

However, it is important to remember that while cyber insurance can provide much-needed financial protection in the event of a ransomware attack, cyber insurance isn't a substitute for cybersecurity measures. It should be used to complement them to ensure the highest possible level of security. Furthermore, even with comprehensive coverage, most policies will not cover all potential costs associated with a severe breach, such as reputational damage or customer lawsuits.

Create a Ransomware Incident Response Plan

Ransomware attacks can be a major headache for businesses, with data being held hostage and disruption to operations. Having an effective ransomware incident response plan in place can dramatically reduce the cost and downtime of a cyber attack and ensure that hasty decisions are not made that impact the ability to perform a post-incident investigation.

A Ransomware Incident Response Plan should cover all aspects of the attack, from initial detection and containment to recovery and remediation. A well-thought-out plan should include procedures for alerting key stakeholders, identifying affected systems, investigating the source of the attack, restoring lost or encrypted data, assessing damage incurred by the attack, and taking measures to prevent future attacks. It's also important to consider communication strategies when developing a ransomware incident response plan, as timely notifications are essential in minimizing damage. A comprehensive plan may include input from external parties that will be involved, such as lawyers, a PR firm and your cyber insurance company.

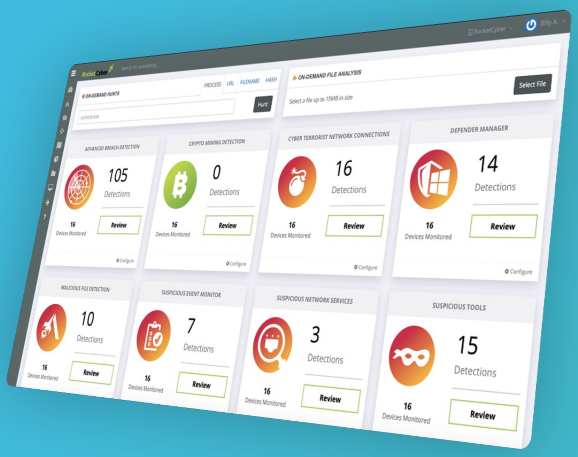
To get our free, full-customizable, Ransomware Incident Response Plan template visit https://www.enterprotect.com/resources/.

Introducing

ENTERPROTECT 360

The Cybersecurity Platform for Busy IT Professionals

Enterprotect 360 is an all-in-one solution that provides powerful protection across your endpoints, network, and cloud - monitored 24/7 by security experts and integrated into a single, easy-to-use console.



Protect Against Ransomware and Zero-day Threats
Multi-layer prevention, protection, detection, and response system stops emerging threats quickly with industry-leading efficacy.

Proactively Reduce Your Cyber Risk
Continuous scanning your endpoints, network, and internet-facing assets for vulnerabilities combined with simple-to-follow remediation guidance backed by support from security experts.

Detect and Eliminate Persistent Threats
Threat Hunting powered by real-time threat intelligence feeds detects, and eliminates, malicious footholds and persistent threats dwelling in your environment.

Add Cyber Experts to Your Arsenal
Extends your workforce with a team of security experts who reduce alert noise, review suspicious activity, and respond to security incidents 24/7.

Detect & Respond to Intrusions and Attacks Quickly
Real-time monitoring of malicious and suspicious activity, identifies attacker TTPs and triggers human response from the Security Operations Center 24x7.

Unified Cybersecurity Dashboard
Single, Cloud-based Cybersecurity Console lets you see all of your cybersecurity in one place, and provides easy access to alerts, tools and reports.

Try Enterprotect 360 including the 24/7/365 Security Operations Center

WWW.ENTERPROTECT.COM/FREE-TRIAL

ENTERPROTECT

Your Cybersecurity Partner

When it comes to cybersecurity, smaller IT teams have the toughest job out there. That's because you have to take care of everything IT-related - in addition to managing cybersecurity.

All too often, there is no one on your team dedicated to security – and even if there is, the bad guys don't clock out, and you/your security person can't work 24/7.

The choice seems to be - to go it alone - or try and get the budget to bulk up your security stack with more (often ineffective) cybersecurity tools.

That's why we created Enterprotect.

Enterprotect combines best-in-class technology and seasoned cybersecurity experts to make the job of managing cybersecurity much easier for smaller IT teams; without breaking the bank.

WWW.ENTERPROTECT.COM

Do you have feedback on this document?

Let us know what you think