datacentrix

Brought to you by:

rubrik

Ransomware Recovery

for dummies®

A Wiley Brand

Develop a recovery plan

Learn how to recover from attacks

Get back to business as fast as possible

Rubrik Special Edition

Michael G. Solomon

About Rubrik

Rubrik helps enterprises achieve data control to drive business resiliency, cloud mobility, and regulatory compliance. Rubrik bridges the gap between owned, on-premises infrastructure, and the cloud by decoupling data from the data center through a software-defined fabric and offering a single management plane for all data, whether on-premises or in the cloud. Comprehensive data management is delivered through instant access, automated orchestration, and enterprise-class data protection and resiliency.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Ransomware Recovery

Rubrik Special Edition

by Michael G. Solomon

for dummies®
A Wiley Brand

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Ransomware Recovery For Dummies®, Rubrik Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2021 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

ISBN 978-1-119-80202-0 (pbk); ISBN 978-1-119-80203-7 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor: Rebecca Senninger

Acquisition Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: William Hull

Production Editor: Mohammed Zafar Ali

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Table of Contents

INTRODUCTION 1
About This Book 1
Foolish Assumptions 2
Icons Used in This Book 2
Beyond This Book 2

CHAPTER 1: **Introducing the Problem of Ransomware** 3
Describing Ransomware and Its Impact on IT 3
Exploring the problem of ransomware 4
Understanding how ransomware affects IT 4
Exploring Real-Life Ransomware Attacks 5
Stopping the Money Changers at Travelex 5
Weathering the storm with the City of Durham, N.C. 5
Examining Ransomware Trends 6
Increasing Resiliency Using Layers of Defense 7

CHAPTER 2: **Preparing to Defend Against Ransomware** 9
Developing a Recovery Plan 9
Assessing your needs 9
Building a plan 10
Testing your plan 10
Protecting the Last Line of Defense 11
Examining the Importance of Backup Immutability 11
Defining immutability 11
Enforcing immutability for backups 11
Recovering Data 12

CHAPTER 3: **Preventing Ransomware Attacks** 13
Understanding Ransomware Vulnerabilities 13
Examining how ransomware attacks computers 14
Tricking a user into infecting a computer 14
Using a shiny object to automatically infect computers 14
Training Users to Avoid Becoming a Victim 15
Recognizing potential attacks 15
Responding to suspicious content 15
Repeating the message 16

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Implementing Security Best Practices 16
Practicing safe user behavior 16
Hardening the IT environment 17

CHAPTER 4: **Identifying a Ransomware Attack and Assessing the Blast Radius** 19
Finding an Attack Sooner Than Later 19
Responding effectively depends on early warning 20
Reducing the recovery workload (and time) 20
Exploring Methods of Detecting Attacks 20
Recognizing ransomware signatures 20
Leveraging machine learning to recognize anomalies 21
Responding to an Attack 21
Preparing the response team 21
Containing the damage and identifying what files were affected 22
Stopping further damage 22
Assessing the blast radius 22

CHAPTER 5: **Recovering Your Data with Surgical Precision** 23
Building a Rapid Recovery plan 23
Backing up is only the first step 24
Assessing recovery time drives recovery success 24
Recovering Only What Is Necessary 25
Focusing on only what you need 25
Eliminating wasted time 25
Automating Recovery at Scale 26
Implementing APIs for unattended recovery 26
Scripting for high performance 26

CHAPTER 6: **Ten Tips to Handling Ransomware Attacks** 27

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

Welcome to *Ransomware Recovery For Dummies,* your guide to learning about ransomware attacks and how to recover from them. Malicious software, called malware, attacks have matured from being annoying to causing business process disruption and even data destruction. A type of malware that is growing in popularity is ransomware. Ransomware gets its name from its behavior. Ransomware encrypts critical files on a victim's computer and demands a ransom be paid for the decryption key. The attacker doesn't actually destroy any data but makes that data unavailable to the victim until the ransom is paid.

The classic advice to best recover from a ransomware attack is to completely restore an affected computer from the most recent backup image. While this approach may sound reasonable, it has its problems. More sophisticated ransomware seeks out backup images and encrypts them as well as the main data. Plus, if you do have a good backup image, restoring a complete environment takes time and may overwrite many transactions. There has to be a better way.

An effective ransomware recovery plan must allow the affected organization to restore normal operations quickly with minimal data loss.

About This Book

Ransomware Recovery For Dummies introduces a sensible approach to recovering quickly from ransomware attacks that you can't avoid. By starting with the threat ransomware poses, you learn how to build a recovery plan that makes sense and keeps your organization safe.

After exploring the ransomware basics, you find out about the importance of a backup solutions provider and what features you need to resist ransomware. You learn how to put the pieces of the ransomware recovery puzzle in place to develop an effective recovery plan. Finally, you review ten top tips for building the most effective ransomware recovery plan.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Foolish Assumptions

I wrote this book based on certain assumptions about you, the reader. First, I assume that whether you're coming from a technical or business side of things you've at least heard of ransomware. Regardless of your role, however, I assume you're interested in finding out more about the threat of ransomware and how to keep it from disrupting your organization's business operations. I also assume you want to know more about the steps you need to take to build a solid ransomware recovery plan.

Icons Used in This Book

Every *For Dummies* book has small images, called icons, sprinkled throughout the margins. I use the following icons in this book:

TIP

This icon guides you to faster, easier ways to perform a task or better ways to put blockchain to use in your enterprise.

WARNING

If you see this icon, proceed with caution. Here you find advice on how to avoid the most common pitfalls.

Beyond This Book

There's only so much about ransomware that can fit in this book. Innovative companies have studied the problem in depth and have come up with some interesting and effective solutions. Rubrik is a leader in providing ransomware recovery services for organizations of every size. For more information about Rubrik's offerings, go to `https://www.rubrik.com/ransomware-investigation`.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Describing what ransomware is and its impact on IT
- Exploring several real ransomware attacks
- Examining ransomware trends
- Using layers to defend against attacks

Chapter 1
Introducing the Problem of Ransomware

Ransomware is a type of malicious software (malware) that encrypts a victim's data and offers the decryption key in exchange for a ransom payment. Ransomware is one of the fastest growing and most feared types of malware. A successful ransomware attack leaves its victims with the choice of losing valuable, sometimes irreplaceable, data or paying a ransom to get it back. As data becomes more valuable to both individuals and businesses, ransomware becomes a greater threat. In this chapter, you find out more about what ransomware is, how it impacts IT, and how you can reduce your risk of becoming a victim.

Describing Ransomware and Its Impact on IT

Ransomware first gained notoriety as a threat to personal data. Most early ransomware attacks focused on individuals and leveraged their increasing reliance on personal data and media. The thought of losing personal pictures, videos, and documents provided enough pressure to convince some victims to pay the ransom. But with every ransom payment, attackers became increasingly emboldened and set their sights on larger targets.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Exploring the problem of ransomware

Today ransomware is a real threat to individuals and businesses. In 2020, ransomware targeted more narrow groups of victims to extract higher ransom payments. For example, according to a recent Emisoft report, "at least 2,354 US governments, healthcare facilities, and schools" were impacted in 2020" (https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/). There is no indication that ransomware is going away anytime soon. Ransomware tactics are becoming more focused and sophisticated.

Attackers have discovered that businesses and critical service providers are often more likely to pay large ransom amounts to end debilitating business interruptions than individuals. Most of today's organizations rely on data and information systems to carry out day-to-day operations. Denying access to critical data is on par with a critical disaster. While many organizations have disaster recovery plans, most don't include proper response to a permanent loss of critical operational data. It's important to understand how the ransomware threat is different from most other threats to avoid facing devastating disruptions to critical business functions.

Understanding how ransomware affects IT

The prospect of permanently losing critical data is a real possibility for ransomware victims. The prevailing attitude is to simply avoid becoming a victim. While that approach sounds good, it only works when it's 100 percent effective. The real question is "how can we recover if any of our preventative controls fail to stop a ransomware attack?" The answer is to implement plans to prevent, assess, and recover.

A good ransomware resilience plan implements multiple layers. Staying safe from ransomware isn't difficult with the right controls and plans in place. There will likely be some changes you must consider for your IT infrastructure. All attackers, and ransomware attackers specifically, depend on "normal" IT infrastructures. They expect to find lots of automation and easy connections to external storage. Surprising attackers with a smarter infrastructure is the first step toward surviving a ransomware attack.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Exploring Real-Life Ransomware Attacks

Before you learn the details of how to prepare for a ransomware attack, take a look at two real organizations that faced ransomware attacks. One was caught by surprise, but the other one had carefully planned for the possibility of a ransomware attack. The second organization not only survived the attack, but continued operations with minimal interruption. The company did it without blowing up its IT budgets, and so can you.

Stopping the Money Changers at Travelex

On New Year's Eve 2019, the London-based company Travelex fell victim to ransomware deployed by the Sodinokibi gang. Travelex, a currency exchange company that operates in 26 countries, found that its core services were severely impacted, backups were deleted, and 5GB of operational data was downloaded and encrypted. The attackers demanded a ransom of $6 million to provide a decryption key and delete the downloaded data. Travelex negotiated with the attackers for several weeks and finally agreed to pay $2.3 million in cryptocurrency to reclaim its data and receive assurance its data would not be publicly released. After paying the ransom, Travelex was able to resume its core operations by the end of January 2020 and return to full operation in February 2020.

WARNING

Make every effort to resist paying any ransom. Each ransom paid increases the attackers' profits and keeps them in business. Paying a ransom can also mark you as an "easy target" for future attacks.

Weathering the storm with the City of Durham, N.C.

Not every ransomware attack ends up costing lots of money or losing lots of data. It's quite possible to plan well and avoid becoming a statistic. The City of Durham, N.C., was the intended victim of a ransomware attack in March 2020. The City of Durham had previously implemented a monitoring and backup infrastructure plan, based on an immutable backup system from Rubrik that ensured their backups were safe from compromise.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

When the attack started, several critical services, including its 911 server, were interrupted. Staff were able to identify the affected files, and recover the files to restore the most critical services quickly. After the most critical services were restored, Durham staff were able to restore all remaining data the attack affected and have all core business systems back online by Monday morning.

Examining Ransomware Trends

Several trends in ransomware have emerged, and none of them is good. Your goal as a steward of your organization's data is to understand threat trends and prepare for potential future attacks. The good news is that in spite of how sophisticated ransomware has become, it's still possible to stay a few steps ahead of the attackers.

Here are some of the current trends in ransomware attacks:

- **Increasing ransom amounts.** Attackers focus their attacks on fewer targets but demand much higher ransom payments.
- **Emerging commodity malware.** You don't have to write malware to use ransomware. Ransomware as a Server (RaaS) vendors make it easy to become a ransomware attacker.
- **Targeting remote work and study situations.** Increasing work and study from home activities, accelerated by COVID-19 restrictions, has resulted in attackers focusing on collaboration and education providers.
- **Exfiltrating data.** In addition to simply encrypting data, some attacks are now transporting data to the attacker's site. After an attacker has a victim's data, that data could be sold for profit or leaked to cause reputational harm or result in legal or regulation violation fines, such as GDPR sanctions.
- **Taking a second pass at extortion.** Exfiltrated data is being used to extort additional ransom payment to avoid releasing sensitive data. Just the threat of releasing sensitive data could be enough to force a victim to pay a ransom.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Searching out and compromising backups.** Many current ransomware variants don't just stop at encrypting local data. They search for any connected data sources and attempt to encrypt all backup copies as well.
- **Continuing rapid growth.** The increased ransom, ease of malware access, and better targeting of victims all result in a growing number of players in the ransomware attacker space looking for profit.

Increasing Resiliency Using Layers of Defense

With a growing ransomware threat of attack and things looking promising for the attackers, it may seem daunting to think about defense. However, a well-thought out defense can prevent many types of ransomware attacks and help you recover quickly from any that may get through your perimeter defenses. The key is to build multiple layers of defense. In general cybersecurity that's called *defense in depth*. It basically just means to put as many controls between your data and an attacker as possible.

Most people think of controls that prevent attack as being the best controls. It's true that preventing an attack is a good thing, but you can't count on preventing every attack. If you don't plan for any possibility of an attack's success you won't be prepared if it does happen.

Preventative controls include personnel training and firewalls. This first layer's goal is to repel most attacks before they get a foothold. Because most malware attacks, including ransomware, start with someone clicking a malicious link, it's important to train your personnel to recognize malicious messages and links. Firewalls can help block obvious traffic, but an authorized user who clicks a malicious link is asking for trouble.

TIP

Even though prevention is important, the real focus to defeat ransomware is on resilience. Knowing what to do if you do suffer a ransomware attack is just as important as knowing how to avoid an attack.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

If an attack does get by any preventative controls, the only way you can respond is to know that an attack is occurring. A strong detection layer is important to provide the ability to take action before it's too late. Monitoring and behavior analysis technology exists today that can provide nearly instantaneous alerts of a ransomware attack in progress.

TIP

You should have real-time monitoring in place for all primary copies of critical data and also have added intelligence on your backup data to provide a last line of defense.

The next layer in your ransomware defense is to stop the attack and identify what damage has been done. You accomplish this by following procedures for disconnecting affected computers from your network and shutting them down. When you reboot them in a controlled environment you can assess the damage. Containerization can make this step easier. Of course, most activities in this layer depend on policies and procedures developed long before an attack commences.

The next layer of defense depends on the backup solution you have chosen to implement. Once you identify the files that have been damaged by the attack, you need to retrieve images of each file before the attack started. Your backup solution should make it easy to recover specific file images from a known point in time quickly.

And finally. Your backup solution will be a prime target for sophisticated ransomware. The only backups you can trust are those with integrity guarantees. Your backup solution must prevent any process, including ransomware, from changing any backup image once it's written to the file system.

If you implement all these layers of defense, you'll have the building blocks in place to recover completely and quickly from any attack that succeeds.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Building your recovery plan
- Ensuring integrity for the last line of defense
- Introducing immutability
- Recovering from an attack

Chapter 2
Preparing to Defend Against Ransomware

Thriving through a ransomware attack is no accident. The only way to avoid becoming a ransomware victim is to plan for an attack and take steps to recover before the attack happens. In this chapter, you find out how to build a plan you can use if you find your company the target of ransomware.

Developing a Recovery Plan

The main problem with ransomware is that recovering from a successful attack is very difficult if you aren't prepared. Even with preparation, recovering without a good plan may not be possible. But don't lose hope; knowing how to develop a good plan could make recovering from a ransomware attack much easier and faster.

Assessing your needs

The first step in planning to survive a ransomware attack is to understand what is important to your organization and what is important to the attackers. A Business Impact Assessment (BIA) is an important process in which you identify the processes that are critical to your organization and what resources support those

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

processes. In short, what does your organization need to be able to do to stay in business?

After you know your organization's requirements to carry out critical business functions (CBFs), you'll have a good idea what data is important to you. For example, an online retailer likely places a high value on its customer and product databases. A library of how-to videos may not be as critical to its day-to-day operations.

After identifying what is important to you, consider what is important to attackers. Attackers generally want to capture data that you value most. In other words, data required by your CBFs. Chances are higher that you'll pay a ransom to get data back you need to stay in business.

Building a plan

Once you understand what data is most critical to your organization (and the attackers), it's time to develop a plan to recover that data if a ransomware attack is successful. You find out more about what to include in your plan in Chapters 4 and 5, but for now, start thinking about who you need on the planning team and how you'll document the plan. You should include representatives from any group of individuals that can influence, or may be affected by, the plan.

Testing your plan

Once you finish your ransomware recovery plan your job isn't done. Unless you fully test the plan you shouldn't fully trust it. The last thing you want to happen is to invest the time and effort into developing a plan only to find out after an attack that a small but critical part was left out. A plan that doesn't work doesn't provide value (or the ability to recover).

You can carry out different types of tests, each one getting closer to a real attack. Most organizations start with checklist tests that consist of stakeholders reviewing the plan together and ensuring all tasks are addressed. A more comprehensive test is a simulation in which stakeholders carry out the actions they would when faced with a real attack. The final type of attack is a destructive attack in which files are actually altered to see whether the recovery team can restore them to a useful state. Of course, the last type of test carries risk, but is also the best test for a recovery plan.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Protecting the Last Line of Defense

Any ransomware that successfully encrypts files relies on the fact that the victim can't access a copy of the affected file. That means the attackers try very hard to find any backup copies of files and encrypt those too. With today's emphasis on automation and connectivity, most backup repositories are easy to find and infect.

Recovering files encrypted by ransomware is a three-step process: 1) Stop the attack. 2) Identify affected files. 3) Recover an unencrypted (pristine) version of the file from a backup.

The third, and most critical, step depends entirely on the assurance that your backups have not been affected by the ransomware. That makes your choice of backup services crucial to recovering from a ransomware attack.

Examining the Importance of Backup Immutability

A successful recovery plan centers on the ability to trust that your backups are pristine. If you can trust that ransomware hasn't altered your backed up files, you can recover from a ransomware attack.

Defining immutability

The critical property that is necessary for ransomware resilience is backup immutability. Immutability means that once you write data it can never be altered. No one, including a ransomware process, can alter data after it was initially written. If you have immutable backups, you have the perfect repository of pre-ransomware data you can use for recovery.

Enforcing immutability for backups

Immutability to support security goals is not a new idea. Logging systems have used immutability for years. Attackers learned long ago that an easy way to cover their tracks and destroy evidence of their crimes was to delete or alter log files. Security professionals quickly realized they needed logging strategies that would allow a service to write a log file entry, but never be able to alter that entry.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Rubrik has developed a unique filesystem from scratch for its backup solution that implements immutability for all files. Backing up a file is easy; you just write it using a Rubrik API call. Once a file is written, it can never be changed. The Rubrik filesystem stores all files natively as immutable, thus they are read-only and doesn't allow any external client on the network to encrypt or delete a stored file. You can read files via an API, but no alterations are allowed. Rubrik's filesystem immutability guarantees that you have pristine files you can use to recover quickly from a ransomware attack.

Recovering Data

Identifying affected files is required before recovering files. While it's true that you could simply recover all files, doing so would dramatically drag out the recovery time. Business continuity focuses on minimizing downtime by only recovering what is necessary to continue business operation.

You took the time to identify the data that is critical to your organization's CBFs. Now determine which of the critical files were encrypted. Depending on the type of ransomware, it may be somewhat easy to identify the files encrypted. Ransomware is just software and needs a register, a manifest, or some other technique to identify encrypted files. After all, the attackers want to be able to decrypt those files after you pay the ransom. (At least that's what they want you to believe.)

WARNING

Most ransomware attackers provide decryption keys after receiving the ransom payment, but trusting a cybercriminal is always risky.

After you identify the file you want to recover, the next step is to carry out the recovery. The best solution is to implement a backup solution that allows you rapid access to backed up files via application programming interfaces (APIs). That way you can write scripts that recover encrypted files quickly and get your organization back in business.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Identifying ransomware vulnerabilities
- Denying ransomware an opening to attack
- Educating users on avoiding ransomware traps
- Adopting best practices to avoid ransomware attacks

Chapter 3
Preventing Ransomware Attacks

Surviving in the era of frequent malware attacks is only possible through a combination of avoiding most attacks and recovering from the rest. Although you must have a robust plan in place to handle successful attacks, the best scenario is when you can avoid the attack altogether. The key to handling any ransomware attack is to first understand the nature of the attack, and then to take measures to prevent the attack, and finally to deal with any attacks that are successful. In this chapter, you find out how to implement measures to avoid ransomware attacks.

Understanding Ransomware Vulnerabilities

Ransomware poses a serious problem, but it isn't an invincible type of malware. Understanding how ransomware works can lead to practices and controls that prevent most ransomware attacks from succeeding. In this section, you find out about some of the vulnerabilities that exist in the ransomware attack plan.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Examining how ransomware attacks computers

Ransomware depends on the ability to run a malicious program on a victim's computer. There are several ways to get the ransomware executable to a victim. The most popular methods are to trick a user into opening a malicious link, navigate to a malicious website, or attach an infected device.

Tricking a user into infecting a computer

By far the most common way for ransomware to infect a computer is for the user to take some action that runs the malicious code. While most users won't deliberately run malicious code on their computers, it isn't hard to trick users into innocently doing the attacker's dirty work. Convincing an authorized user to carry out an action for an unauthorized person is called social engineering.

Most people are vulnerable to social engineering because they want to be helpful, are interested in free stuff, and don't want to get into trouble. Attackers know that they can leverage one or more of these user desires. That's why many ransomware infections start with an unsuspecting user clicking a link on a website or in an email that helps someone out ("Click here to donate to a worthy charity"), satisfies their curiosity ("Click here to claim your cash"), or avoids getting into trouble ("Click here to change your password").

Using a shiny object to automatically infect computers

Ransomware doesn't always require a user to click a link. A drive-by download attack downloads malicious code when a user visits an infected website. Another type of attack consists of dropping infected USB keys at physical locations where people are likely to notice them. The first thing most people do when they get a free USB key is to insert it into a computer to see what it contains. For infected USB keys, the act of inserting it into a computer is all that it takes to copy and launch the ransomware.

WARNING

Many types of attackers use the USB key trick to plant malware. Don't blindly trust USB keys from any unknown source, including those given out for free at meetings and conventions.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Training Users to Avoid Becoming a Victim

One of the best investments any organization can make to avoid ransomware is end user training. Users provide nearly all the entry points for successful ransomware attacks and play a vital role in stopping attacks before they start. Training users to recognize potential attacks and resist the temptation to click questionable links can result in a much lower probability of attack success.

Avoid focusing your end user security awareness training on only what users should and shouldn't do. In addition to specific acceptable use training, make a point of your training to enlist users as security operatives. Security is everyone's responsibility, not just a small group of security specialists. Let all personnel know that good security is a team effort, and everyone needs to be diligent. One careless mistake can expose an entire organization to attack, so everyone must pitch in to defeat the attackers.

TIP

Giving users ownership of the organization's security can go a long way toward eliminating careless actions that lead to a breach.

Recognizing potential attacks

Because users provide a ransomware entry point so frequently, a sure way to reduce the attack potential is to teach users to be attentive and to recognize suspicious content. Show users examples of phishing emails and provide guidelines on how to identify a potential attack.

Phishing emails are becoming more and more sophisticated, but most are easy to spot. Include tips for users to identify emails that may be malicious. Teach them to pay attention to grammar (does the message make sense?), salutations (are you addressed by name), and specific content (does the message contain details or is it generic?) that can make malicious messages stick out. Once users know what to look for, they can play a part in preventing attacks.

Responding to suspicious content

Recognizing suspicious content is a good start, but users also need to know what to do next. Your organization should have a specific place to report suspicious email messages, other media,

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

or behavior. For email messages, users should forward anything that looks odd to a specific email address. Your security personnel should monitor that email address and examine any reported messages. At first you may find that users forward many messages to the monitored email address. However, if your security personnel respond with an explanation of whether the message was malicious and why, users learn more about suspicious messages and the number of false alarms should go down.

Repeating the message

It would be great if security awareness training "stuck" forever, but it unfortunately doesn't happen that way. Users forget how important security is, they get busy with deadlines, and they get weary of always being diligent. One consistent characteristic of successful security awareness programs is their ongoing nature.

Instead of only offering security awareness training once, you should require recurrent periodic training. Also, mix up the delivery style. A monthly or quarterly "Lunch and Learn" series often works better than an annual half day session. The goal should be to keep reminding personnel of their role in security and how to best fill that role.

Implementing Security Best Practices

Instead of trying to reinvent the wheel, a great place to start when building a security plan is with well-established best practices. Fortunately, many organizations have found some tried and true best practices to be helpful in preventing ransomware attacks. You won't find a single repository of best practices, so this section lists some of the most useful actions an organization can take to prevent ransomware attacks.

Practicing safe user behavior

Once your personnel understand how ransomware works, they're more likely to accept guidelines for online behavior. Users can do (or avoid) many things that make the IT environment safer and less prone to ransomware attacks. Here are some actions users can do to stay safe:

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Verify email senders before opening a message.
- Don't open attachments unless you trust the sender.
- Don't open unexpected attachments.
- Don't follow links in email messages.
- Don't respond to suspicious looking messages.
- Forward any suspicious messages to your security group.
- Only visit websites you trust.
- Don't provide personal information unless you trust the website, the reason the data is needed, and only for interactions you initiated.
- Don't attach/insert/mount an external device (such as a USB key) unless you trust its source.
- Always use a virtual private network when connecting from a remote location.
- Keep your software and operating system patched and up to date.

Following these best practices will make it difficult for any attacker to launch a successful ransomware attack.

Hardening the IT environment

IT and security personnel also have best practices. Implementing the following best practices help provide and maintain a more secure environment for your users.

- Identify all critical data.
- Create periodic backup copies of all critical data.
- Develop and test a comprehensive recovery plan.
- Update all computers and devices with the latest security patches.
- Require a virtual private network for all remote access.
- Require antivirus/antimalware software on all computers and devices.
- Implement malware scanning and filtering on mail servers.
- Implement firewalls with restrictive rulesets at each trust boundary.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Conduct ongoing security awareness training for all personnel.
- Establish, publicize, and staff a support function to investigate reported suspicious messages or websites.

While no amount of prevention is 100 percent effective, every little bit helps. Every ransomware attack you prevent is one from which you don't have to recover. The best strategy is to prevent every attack that you can, and prepare to recover from any attack that is successful.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Identifying an attack as it's happening
- Alerting the right people to respond to an attack
- Assessing the extent of an attack's damage

Chapter 4
Identifying a Ransomware Attack and Assessing the Blast Radius

Despite your best efforts to prevent every ransomware attack, a successful attack is still possible. In this chapter, you find out how to identify a ransomware attack as soon as it starts and how to assess the extent of the damage.

Finding an Attack Sooner Than Later

A ransomware attack succeeds by infecting one or more systems, finding critical files, and then encrypting them. Because it takes time to encrypt files, the earlier you detect and stop the attack, the fewer files you must recover.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Responding effectively depends on early warning

As with any type of attack (cyber or otherwise), early detection makes it possible to contain the damage and recover faster. If the attacker can't do as much damage as they'd like, you'll have less to clean up if you get involved early.

Early involvement in the recovery effort depends entirely on your early warning system. Unfortunately, over half of reported and analyzed ransomware in a recent study weren't discovered for more than a month. That means the attack had weeks to do what they wanted in a majority of cases. You don't want to be part of that statistic.

Reducing the recovery workload (and time)

Even if you detect an attack in well under a month you could have a lot of work ahead of you. As the seconds tick by during an attack more files get encrypted. Early warning and quick response can dramatically reduce the scope of recovery work. And having to recover fewer files means you'll be up and running faster than if you wait too long to respond.

Exploring Methods of Detecting Attacks

Ransomware software activities aren't the same as normal operations. While other applications do encrypt files, ransomware encrypts many files in a short period of time. Recognizing a ransomware attack depends on recognizing unusual behavior or changes. In this section, you find out about two approaches to detecting ransomware attacks.

Recognizing ransomware signatures

One approach to ransomware detection is an extension of general malware detection. It isn't hard to detect known malware by comparing a portion of an executable program's code with a database of code signatures. If you find a match, you've probably found a malware program. Ransomware signature matching works in the same way. The main drawback to this approach is that you must keep your signature databases updated to the

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

very latest signatures and any completely new or slightly modified ransomware will be missed. A new attack won't be detected until someone reports it and its signature gets added to the next release of the signature database.

WARNING

One of the disadvantages to signature matching is ransomware is getting smarter and evolving rapidly so there are new signatures all the time.

Leveraging machine learning to recognize anomalies

Another approach to detecting malicious behavior is to use machine learning (ML) algorithms to compare normal behavior and filesystem state to current behavior. ML algorithms are very good at learning what "normal" looks like and flagging any behavior that looks abnormal. ML algorithms can look at running processes and the resources they're using, as well as unusual changes to the filesystem.

For example, the Rubrik Ransomware Investigation application uses ML to analyze filesystem changes. Ransomware Investigation looks at the type and frequency of changes, as well as for signs of encryption and file entropy changes. Ransomware Investigation can provide alerts of unusual behavior as an added layer of intelligence.

TIP

Your first line of defense should be any of a number of real-time detection and monitoring tools to catch suspicious changes early.

Responding to an Attack

Responding to any security incident, including a detected ransomware attack, should simply be following your response plan. Of course, that means you have to have a plan and a trained team in place to make it happen.

Preparing the response team

Long before your response team is ready to recover from a ransomware attack you must assemble and train the response team. The ransomware response team may be the same team that

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

responds to other security incidents, but it needs to have special training for ransomware response. The key is that you build the team, train the team, and have your team carry out response plan tests to ensure they're ready.

Containing the damage and identifying what files were affected

Once you've initiated your ransomware recovery process, it's time to get busy. The main goals are to stop the attack and any further damage, and then restore any affected computers and files to an operation state. The first phase of recovery is to contain the attack's damage and assess how much damage has already occurred.

Stopping further damage

The response team should already have a good idea of which computers are participating in the attack. Their first action should be to stop the ransomware processes, generally by shutting down any affected computers. The next step is to check whether other computers are active participants in the attack and shut them down as well.

You can bring the affected computers back up disconnecting them from all networks. That gives you the ability to access the computers and storage devices to remove the ransomware.

Assessing the blast radius

Once you've stopped the attack you can assess the damage. The scope of the damage already done is often referred to as the blast radius. The blast radius is defined for a ransomware attack as the collection of files that have been modified in the attack. Most ransomware adds or changes the filename extension as it encrypts each file, making identifying damaged files easier. Some ransomware builds a manifest as it encrypts files. Either way, you should be able to determine how big your blast radius is. Blast radius is related to attack time — the longer you wait, the more damage you have to clean up.

Assessing the blast radius prepares you for the next step — the recovery. If you have planned well for a ransomware attack and protected backed up files, recovery should be straightforward.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Developing a plan to meet your recovery goals
- Limiting the recovery process to only what you need
- Automating recovery for speed and reliability
- Enabling multiple defense layers for a seamless ransomware response

Chapter 5
Recovering Your Data with Surgical Precision

Once you've detected an attack, stopped the damage, and identified what files have been affected, it's time to trigger your recovery plan. A good recovery plan makes getting back to normal operation as quick and painless as possible. Precision and speed are the keys to a fast and reliable recovery. In this chapter, you find out how to build, test, and follow a ransomware recovery plan that will protect you from any ransomware threat.

Building a Rapid Recovery plan

The key to recovering from a ransomware attack is having the flexibility to recover files in a granular fashion. Granular recovery means that you can fetch copies of the files affected by the attack before the ransomware encrypted them, without having to restore all backed up files. Once you know which files you need to recover, the rest of the plan is executing the steps to recover those files.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Backing up is only the first step

A good backup strategy is the foundation of ransomware recovery, but the plan doesn't stop there. Backups you can trust and use to recover from a ransomware attack must guarantee immutability and provide easy access to authorized individuals. You must build a plan that provides detailed and simple procedures for recovering a list of files. The plan should provide guidance for developing the recovery actions and estimating the time required for recovery.

One of the most important parts of a recovery plan is its assessment requirements. Every recovery plan should include guidelines for methods and frequency of testing the plan.

TIP

Never trust an untested plan. Tests should be recurring and of different intensity levels, from simple readthroughs up to full failure recovery. The closer you move toward full failure testing the risk increases, so you must carefully plan how you test your recovery plan without introducing excessive risk. It isn't difficult to recover files to a non-production environment first to prove the recovery procedures' validity. Then you could recover non-critical files to a production environment before carrying out a full interruption recovery test.

Assessing recovery time drives recovery success

An important business requirement of any recovery plan is meeting the organization's recovery time objective (RTO). Your recovery plan must restore the organization to a recovery point objective (RPO) within the RTO. The RPO defines what conditions you must meet to restore CBFs and continue normal operation.

Put another way, your recovery plan must restore operations as defined by the RPO and do it before the RTO time limit elapses. If the recovery process takes longer than the RTO, your business processes will suffer. Think of the RPO and RTO as constraints that limit how much you should do and how long you can take to recover. Doing more than meeting the RPO will almost always risk exceeding the RTO.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Recovering Only What Is Necessary

Many ransomware recovery plans are based on restoring entire computers. Whether you use virtualization and checkpoints or a full backup image to restore a computer, you're painting with a very wide brush. A ransomware attack doesn't encrypt every file so you shouldn't restore every file to recover. In this section, you find a better way to avoid extra work and time to recover.

Focusing on only what you need

A heavy-handed approach to ransomware attack recovery could add additional damage to the attack. You only need to recover the files encrypted by the ransomware, so why restore anything else?

Normal day-to-day business functions routinely change data. Many of these changes are coordinated across multiple files, databases, or even computers. Any operation that overwrites data changes by restoring an earlier version of data effectively "undoes" changes. If you restore files that weren't affected by a ransomware attack you may lose transactions or even get out of sync with other systems.

For example, suppose your organization sells pet supplies online. A ransomware attack started encrypting Microsoft Word and Adobe Acrobat documents on your order processing server. You detected the attack after several hours and followed an old ransomware recovery procedure. The outdated procedure directed the incident response team to shut down the computer and restore everything to a point in time before the attack. Instead of just recovering the affected files, you eliminated all orders that were taken since the attack started and orphaned all orders that had already been sent to your shipping department. Your billing department is unhappy because of the mess your "recovery" has created.

TIP

A far better approach would be to incorporate a multi-layered service such as Rubrik's recovery services into a recovery plan that can make it easy to recover only what you need.

Eliminating wasted time

In addition to avoiding a recovery operation that overwrites too much data, recovering only what you need is faster. Well, if your backup solution provider exposes APIs to make specific file

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

recovery easy then recovering just what you need is fast and easy. Rubrik provides you with the ability to identify what files were affected and restore only affected files from a trusted, immutable backup repository to a state before the ransomware attack.

Automating Recovery at Scale

The final key to a smooth ransomware recovery process is the ability to automate the repetitive and redundant actions. If you have 10,000 files that an attack encrypted, automating the restore process for all files makes the process more dependable and faster. In this section, you find out how Rubrik supports fast and effective file restoration through automation.

Implementing APIs for unattended recovery

Rubrik provides APIs to access and retrieve files from its immutable backup file system. The Rubrik APIs provide secure access to your files on demand and by any host language. You can write software to access your files in your favorite language. Rubrik doesn't impose an inflexible user interface as the only way to access your data. It's your data. You can access it; however, you want to use the flexible and secure APIs.

Scripting for high performance

The Rubrik APIs for data access provide the icing on the cake for ransomware recovery. Once you identify a list of files the ransomware attack encrypted, you can write a script in your favorite scripting language to carry out the restore. For each file in your list, all you need to do is query your backup data using Rubrik's API to find the last backup version before the attack, and then call another API to restore it. Your scripts, supported by Rubrik's systems, will restore your organization to an operational status quickly and efficiently.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Chapter 6
Ten Tips to Handling Ransomware Attacks

After learning about ransomware, it may seem that surviving an attack is a daunting task. However, once you understand the attacks, how to avoid them, and how to recover from them, planning to confront ransomware can be a straightforward project. This list gives you ten tips to putting a plan together to not only survive but thrive in the face of a ransomware attack.

- **Train users to avoid ransomware attacks.** Train all users on how to recognize common ransomware attacks and how to avoid becoming a victim. Provide a method for users to report suspicious messages or websites and train users how to report anything suspicious.
- **Turn on mail server filtering.** Today's mail servers either include options or support add-ons to filter mail messages and attachments for suspicious content. Research how to enable this feature for your mail server and use it.
- **Identify critical files.** Take inventory of your organization's critical business functions and the data each one needs to operate. Create a manifest of files that are critical to your organization staying in business. This list of files should be the focus of your protection and recovery efforts.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Choose the right backup service provider.** Choose a backup service provider that can guarantee immutable backups and easy access to unencrypted files via flexible but secure APIs. Both of these features are integral to Rubrik's service offering design.
- **Back up critical files to an immutable destination.** Frequently back up all the files on your critical files manifest to a backup service provider that guarantees immutability, such as Rubrik, to ensure ransomware can't encrypt your backups.
- **Develop a plan to recover files.** While backing up critical files is a great first step, develop a formal plan for recovering files if a recovery process is needed. Document the conditions under which you should recover, who will carry out the recovery operations, how to identify what to recover, and how to recover identified files.
- **Create automation templates for quick recovery.** When you need to activate your plan, all you should need to provide is a list of files to recover. That means part of your plan should include script templates to carry out the recovery process for any list of files. Script templates give you the ability to test the recovery process many times and fine-tune the process operation.
- **Test your plan frequently.** In addition to testing individual scripts, it's important to test the entire recovery plan frequently. The only valid plan is one that meets your RPO and RTO requirements. Ensure all participating personnel are comfortable with their roles and the plan flow. Frequent tests validate the plan's effectiveness in changing environments and keeps personnel fresh and ready to go.
- **Monitor critical files for suspicious changes.** Implement file integrity monitoring on production filesystems to detect suspicious changes, such as those consistent with ransomware. As an added layer of protection, implement similar monitoring for backup locations. Any unauthorized backup changes or unusual changes to previously backed up files should be noted. Ensure your backup service provider delivers alerts for suspicious backup changes.
- **Train and deploy an incident response team.** Assemble a team of personnel with the express purpose of responding to a suspected ransomware attack. The team should be fully versed in the recovery plan and be comfortable with their clearly defined roles. Ensure each team member participates in frequent tests to keep everyone ready to respond whenever the demand arises.

These materials are © 2021 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Recover faster from ransomware

Businesses are run on data these days, and as it's become more valuable, ransomware has become a real threat. One you can't afford to ignore. The key to thwarting attacks is knowledge. Knowledge about how ransomware works and how to get up and running after an attack. *Ransomware Recovery For Dummies* shows you how, when, and where ransomware can attack, and the steps your organization can take for preparing for an attack, assessing impact, and recovering quickly should an attack occur.

Inside…

- Learn about ransomware attack vectors
- Employ a defense in depth strategy
- Ensure security with user training
- Access damage after an attack
- Restore operations quickly with minimal data loss

Michael G. Solomon, PhD, is a cybersecurity consultant who provides executive level guidance to help clients align compliance requirements with strategic goals. Dr. Solomon is a Professor at the University of the Cumberlands and holds a PhD in Computer Science and Informatics from Emory University

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-80202-0
Not For Resale

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.