daisy.

HOW TO BEST PREPARE **FOR RANSOMWARE**

Tips and advice on how to avoid becoming a ransomware victim

WHAT IS RANSOMWARE?

Cyberattacks are getting more sophisticated and are holding organisations hostage until they pay millions in ransom. The reality is that you either pay the ransom or you keep an offline copy of data that is disconnected from the network to restore your production environment.

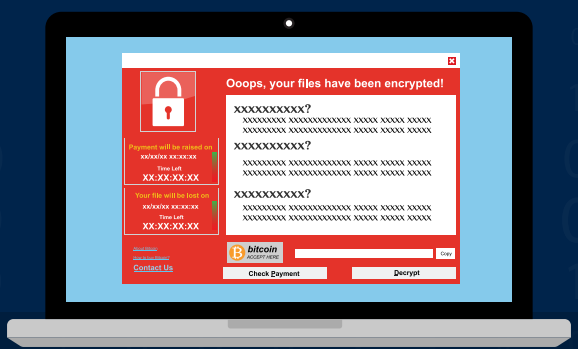
Ransomware is a type of malicious software that prevents users from accessing their systems or data. A sum of money is demanded to be paid in return for the decryption key under the threat that data will be made public or continue to be withheld until the ransom is paid.

Ransomware is here to stay. Rather than just hoping it won't affect you, read this guide for useful options that exist to help.

48%
of organisations were hit by a ransomware attack last year

13%
of those reportedly paid the ransom

SOURCE: SOPHOS



ARE NEW RANSOMWARE REGULATIONS ON THEIR WAY TO THE UK?

Demand for ransomware payments has increased during the COVID-19 pandemic, leading to a new advisory (October 2020) from the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). It warns that companies that facilitate ransomware payments to cyber actors on behalf of victims may risk violating its regulations.

The advisory says facilitating a ransomware payment that is demanded as a result of malicious cyber activities may enable sanctioned persons or jurisdictions to fund illicit activities and undermine the national security and foreign policy objectives of the US. Government agencies could impose fines on organisations that pay the ransom to get their data back, and this could prompt other countries to take a similar stance.

HOW CAN YOU HELP PREVENT A RANSOMWARE ATTACK?

Steve Burden,
Security Product Manager,
Daisy Corporate Services

"The problem with ransomware is that once you have it you can't do anything to stop it. Unless you've got appropriate backups, you are at the mercy of the perpetrator. This means that from a security perspective, it's more about stopping it happening rather than fixing it once it's happened. There's no one thing that is guaranteed to stop it happening. The best approach is to have multiple layers, all of which you would hope to catch it en route. The most relevant would probably be a combination of web security, email security, firewalls and antivirus software.

You might also deploy a security information and event management (SIEM) platform with the intention of discovering a ransomware attack in time to isolate that machine from the network and therefore stopping it from spreading to other devices.

We know a fair bit about how and where ransomware attacks manage to penetrate customer environments, so make sure you've got the basics covered as a starting point."

MAKE SURE YOU'VE GOT THE BASICS COVERED

It was reported at the start of this year that...

more than **57%** of ransomware attack vectors were via a remote desktop protocol (RDP) compromise

more than **26%** were via phishing attacks

and more than **12%** were from software vulnerabilities

SOURCE: VEEAM

Knowing this, is a huge help in focusing the scope of where to invest the most effort to be resilient against ransomware from an attack vector perspective.

For RDP desktop access -this is an opportunity to for IT administrators to refine security access – ensuring servers are not directly connected on the Internet is essential in starting to develop a forward-thinking ransomware resiliency strategy.

For phishing - we all know that users are regularly targeted with spam emails and there is a requirement to educate and inform all staff members and add warnings to emails that originate outside of your organisation. Gophish and KnowBe4 are useful tools to help you understand where training is required.

For software vulnerabilities - keeping systems up to date is a tedious task, yet it is now more important than ever, as we know that ransomware attacks exploit known vulnerabilities. Also, keep in mind the need to stay current with updates and upgrades to critical categories of IT assets: operating systems, applications, databases and device firmware.

HOW CAN YOU BEAT A RANSOMWARE ATTACK?

Mark Wilson,
Business Continuity Solutions Architect,
Daisy Corporate Services

"For a ransomware attack to work, your organisation's security has to be breached in the first instance, but this on its own is not enough to bring the organisation to its knees. Once access to your infrastructure has been gained, the intruder also needs to be able to prevent you from accessing your own data. If you take even some basic steps to protect your data, for example, leveraging offline, air gapped and immutable backup technologies, you can recover to a point in time prior to any attack.

If you can recover your uncompromised data safely and easily and continue your normal business operations, the criminals don't have any hold over you."

THE OFFLINE RULE

At any given time, are one or more of your backups offline?

The purpose of an 'offline backup' is that it remains unaffected should any incident impact your live environment.

You can ensure an offline backup by:

- only connecting the backup to live systems when absolutely necessary
- never having all backups connected at the same time

With at least one backup offline at any given time, an incident cannot affect all of your backups simultaneously.

AIR GAPPED STORAGE

Is your backup data completely separate?

Air gapping is a network security measure that ensures a secure computer network or device is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network.

IMMUTABLE DATA

Is your data in a state that cannot change?

Once it is backed up, it cannot be edited or modified so it is a true point-in-time copy of your data.

To achieve air gapping and immutability, you don't have to resort to tape backups or even virtual tape libraries on specialised hard disk backup storage. All you need is object storage that supports immutability, such as that provided by Daisy with our Veeam solution.

FLEXIBLE RECOVERY OPTIONS

In any cyberattack it is important to have flexible recovery options so that you can recover your data wherever it is safe to do so, and so that it cannot be impacted, infected or compromised by connections at any stage.

SAFE HAVEN

If the worst comes to the worst, you may need to go completely off-grid, with a new physical environment for your staff as well as clean IT equipment and data. Daisy's Safe Haven service allows you to replicate some or all of your IT infrastructure and staff locations, to address the nature of the breach and the unique requirements of your business.

Daisy can help you to get into the best possible shape for fending off a ransomware attack.

Call us on 0344 863 3000

or visit dcs.tech/ebackup

bci Founding Partner

VEEAM CSPPARTNER Platinum

bsi. ISO 22301 Business Continuity Management BCMS 563370

we are daisy.

dcs.tech