NOVI

Technology for Business

Whitepaper

Ransomware: What it is and how to prevent it

e. hello@novi.ie t. +353 (0) 1 621 8633 novi.ie

Ransomware: What it is and how to prevent it

What is Ransomware?

Ransomware is a sophisticated malware attack that takes advantage of security vulnerabilities in computer and server operating systems. Ransomware then encrypts all files on server file shares making them completely inaccessible.

The cybercriminals then demand a ransom request, normally payable in bitcoins, to provide you with the code to decrypt the files and make them accessible again.

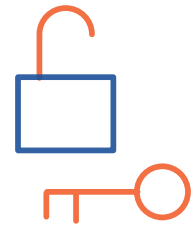
Ransomware is big business for cyber criminals who can now purchase it as a service that they use to target businesses. In some instances, the service itself is free to purchase with the profits from the ransom demands then split 50/50! With this service anyone with limited IT expertise can set themselves up as a hacker.

What if I ignore the ransom request?

Ransom requests tend to come with a deadline, if the ransom request goes unpaid within that timeframe the ransom increases. It is however possible in most cases to recover files and restore service from the last good backup or server image, but this can take a significant amount of time with systems inaccessible during that time. However, if you do not have a good backup system in place and you decide not to pay the ransom you will not be able to unencrypt and access the files.

> Only 39% of Irish companies have a fully operational incident response plan to deal with security breaches, while 28% had no plan at all.

Ransomware:
What it is and how to prevent it



What happens if I pay the ransom?

When you pay the Ransom, you are typically provided with a code that unlocks your encrypted files.

Caution: **Ransomware often returns a second time (and third) to those who do not take the necessary precautions after the first occurrence.**

> The frequency of cyber-attacks against Irish businesses has risen from 25% in 2012 to 44% in 2016.

How does a cyber-criminal choose my business?

Every organisation and every individual leaves a digital footprint online, with which a cyber-criminal can profile your business, putting together information such as number of employees, contact details and personal details, often easily found through social media accounts. Cyber criminals can easily collect what look like insignificant pieces of information to generate a much bigger picture about your business.

This profile or detail about your organisation is very valuable. While some criminals will collect the data and sell it on to those that compile marketing databases or to more sophisticated criminals, many will use it to target you directly. A Phishing email, carefully created using knowledge about you and your business to manipulate your trust, is then sent to make contact.

The majority of scams take advantage of our trusting nature as humans, whereby people are deceived into revealing information that contribute to the profile, and ultimately into clicking on a link that allows malware to infect their machine and cyber-criminals to gain entry to the organisation's network.

How does Ransomware spread?

Like most malware attacks, Ransomware most often depends on human interaction to download the malicious code without their knowledge. Malware is typically spread by email, embedded in attachments such as ZIP files or URL links within PDF attachments. When attachments are opened or clicked, the code can then take advantage of any security vulnerability in computer and server operating systems.

> Nearly a quarter (23%) of Irish organisations have been held to ransom by a hacker, and yet the vast majority (93%) assert they would never pay a ransom.

How do we protect our business data and systems from Ransomware?

Organisations often overlook the basics when it comes to protecting themselves from cyber security activity, and Ransomware is no different. Security is all about awareness and implementing several layers or protection (not just antivirus) to help prevent or minimise the chances of a cyber-security related attack. Remember, these attacks are primarily random which means that both small and large businesses are vulnerable. If you do not have the expertise in house, our advice is to look for help from a managed services provider with strong security expertise.

Ransomware:
What it is and how to prevent it

Here are five tips every business should look to implement to protect against Ransomware:

1. Keep operating systems patched and firmware updated. Treat this as essential proactive maintenance that must be carried out routinely. Do not depend on automatic updates to assume this is being done correctly. If you do not have the time or expertise, outsource this to a managed services/security provider.
2. Educate employees, as human error is often the biggest weakness when it comes to cyber security. Facilitate brief classroom type sessions that present examples of phishing emails and encourage questions and participation from employees.
3. Ensure you have a unified threat management (UTM) firewall in place and that it is properly configured as most firewalls installed today are not sophisticated enough or correctly configured to prevent attacks.
4. Ensure you have a working backup and imaging solution in place that you can confidently recover information in the event of an attack.
5. Ensure you have email protection in place. In fact, major security vendors are recommending that multiple layers of email filtering may now be necessary to keep up with the level of sophisticated email attacks.

Why it is vital to monitor cyber activity

Many cyber-attacks sit undetected in networks as criminals have invented smarter methods to stay hidden. Organisations may not yet know they have been a victim of a cyber-attack, but the destructive effects appear as it becomes apparent an attack took place.

Until recently, a typical network diagram consisted of a firewall with external untrusted networks shown outside the firewall and internal “trusted networks” and “trusted devices” shown behind the firewall.

Today, the approach to network design needs to be very different. Every network and device, including those internal to the organisation, need to be considered “untrusted” and, as such, treated with suspicion. The evolving threat is forcing organisations to rethink the entire internal structure of their own networks right back to the core in an effort to protect themselves.

Internal Segmentation Firewalling (ISFW) is a more modern approach to localising potential threats than a core UTM (unified threat management) scan as it inspects internal traffic when it passes from one internal network to another. The goal is to minimise the spread of attacks from compromised devices and protect sensitive company data and mission critical systems.

It is essential that businesses measure and understand cyber security activity inside their own organisation. Cyber security monitoring and internet reporting help create a vital security benchmark and offer actionable intelligence such as identifying malware infected devices inside the network that would otherwise go unnoticed.

> With 200,000 new pieces of malware identified every day going undetected for an average 210 days, prevention is the best cure

Adopting a risk based approach

Those responsible for an organisation's security measures can often feel overwhelmed and struggle to determine what they should protect and how. A risk based approach can help security officers focus their resources helping them identify where the biggest risks lie.

The obvious first step is to identify what the most valuable data is and where it is stored. Every department may differ on what data they deem to be most valuable. An internal audit or workshop with the help of an IT security consultant will help prioritise and identify the high risk data.

The workshop should focus on the following:

1. Identification of the information, e.g. medical records, intellectual property, personal HR information.
2. Identification of where the information is stored and how people interact with that information.
3. Classification of the data into categories such as 'public information' (requires least protection), right up to 'highly sensitive' (requires most protection).

Once you create such a matrix, a threat modelling exercise will help determine the probability of various threats and the impact to the organisation if such a threat occurred.

For example, threats could consist of spoofing of identity, data tampering, denial of service, or data loss. The modelling exercise would enable you to score each individual data category and help form the business case for investment in the required technology, processes and people to support your findings.

It is important for information security offices not to get distracted by continuously chasing new tools when overlooking the basics such as proactively patching and maintaining systems that might otherwise make them vulnerable.

Do not overlook people in your organisation, as they are the biggest threat. It is important to ensure that privileged access to information is monitored and that anomalies can be identified. Ensure that security processes and incident plans are in place and followed.

About the Author

George O'Dowd is MD and founder of Novi Technology. Novi has been supporting business IT systems since 1999.

Novi's uniquely comprehensive service delivers traditional IT Managed Services along with advanced security protection. Through regular, scheduled onsite visits, coupled with proactive 24/7 network monitoring and sophisticated data analytics, Novi detects issues before they become a problem, reducing unplanned system outages by a massive 70% and reducing the risk of a cyber breach by up to 93%.

George O'Dowd MD