Hewlett Packard Enterprise

OWNERS MUST PROTECT THEIR BUSINESSES FROM RANSOMWARE BEFORE IT'S TOO LATE!

SHOCKING FACTS ABOUT RANSOMWARE

- Ransomware is projected to attack one business every 14 seconds by the end of 2019, up from every 40 seconds in 2018.

  Source: Cybersecurity Ventures, 2019

- 1.5 million new phishing sites are created every month by criminals.

  Source: Webroot, 2017

- The average time taken to recover from a ransomware attack is now 16 days.

  Source: Coveware, 2019

- Ransomware cost US businesses more than $7.5 billion in 2019

  Source: Emisoft, 2019

- 60% of SMBs hit by ransomware fold within six months

  Source: US National Cyber Security Alliance

RANSOMWARE IN ACTION

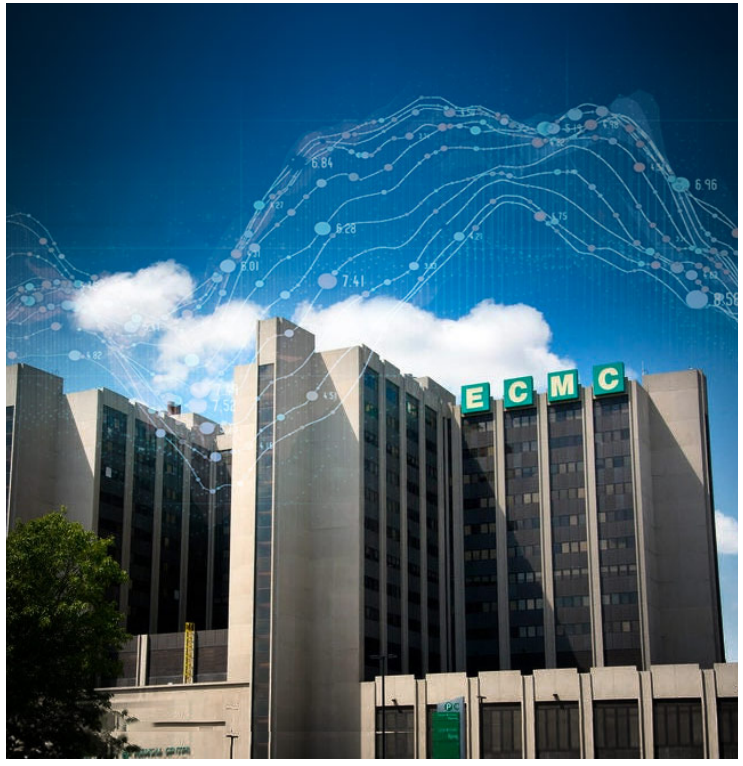
Danish transportation and logistics giant Maersk suffered $300M of business interruption losses due to a ransomware attack. The recovery effort required Maersk to re-install 4000 servers, 45,000 PCs, and 2500 applications over ten days.

British pharmaceutical company Reckitt Benckiser estimated that its victimization by the NotPetya ransomware cost it $140M dollars in disrupted production.

RANSOMWARE IN ACTION

Tech vendor Nuance recently reported that a ransomware attack it suffered in the fall of 2017 cost it $68M in refunds to customers for service disruptions and another $24M in cleanup costs.

South Korean web hoster Nayana was affected by the WannaCry outbreak, and ended up paying $1M in Bitcoin ransomware to regain access to 150 servers and restore web services to 3400 customers.



Erie County Medical Center (New York, USA), which lost access to 6000 computers, requiring six weeks of manual operations and a recovery process that ultimately cost US$10M.

SO RANSOMWARE IS A MULTIBILLION-DOLLAR A YEAR BUSINESS

Ransomware is the first type of malware that actually generates revenue for the attacker. Companies hit by a ransomware attack are forced to pay a “ransom” – anywhere from hundreds to thousands of dollars – to “unlock” the files that have been maliciously encrypted. Ransoms can range from $5,000 to $50,000 and beyond depending on the size of company.

BECAUSE IT'S A PROVEN SUCCESSFUL BUSINESS MODEL FOR ATTACKERS

2019 has already seen a spike in ransomware attacks hitting large companies and government agencies, crippling public services and causing major disruptions. There are countless others – assaults that hit small businesses – that never make the news, but still have a devastating effect.

BECAUSE IT'S A PROVEN SUCCESSFUL BUSINESS MODEL FOR ATTACKERS

Ransomware as a service is now a fact; criminals can buy ransomware kits 'off the shelf' to use in their extortion attempts – in some cases for as little as $25.

BECAUSE IT'S A PROVEN SUCCESSFUL BUSINESS MODEL FOR ATTACKERS

Even if companies pay the ransom (not recommended) it can take days or weeks to implement the hundreds or thousands of encryption keys that unlock their data. Around 30% of companies lost access for at least 5 days. It took the city of Atlanta weeks to fully recover.

SO WHAT CAN BUSINESS OWNERS DO TO PROTECT THEMSELVES?

- Make sure your security software is up to date.
- Make sure you're running the most recent versions of all your operating systems and patch and update applications.
- Educate end users.
- Have a robust backup process in place – utilise the 3-2-1-1 rule.
- Use LTO Ultrium tape to create an air gap.

WHAT IS THE 3-2-1-1 RULE AND HOW DOES IT HELP?

THREE COPIES OF YOUR DATA

TWO DIFFERENT MEDIA TYPES

ONE STORED OFF SITE

ONE OFFLINE BEHIND AIR GAP

RANSOMWARE ATTACKS HAPPEN EVERY 40 SECONDS

BUT IT'S NOT JUST RANSOMWARE

- Digital data is vulnerable to a number of pervasive threats.
- Tape is not just a ransomware antidote.
- Having a last line of defence addresses a number of vulnerabilities for data.
- Not all disasters are malicious – having your data safe behind an air gap and off premises can be an excellent defence against disruption caused by natural disasters, like hurricanes, floods and fires.

LTO ENCRYPTION – WHERE YOU HAVE THE KEY!

1. In a ransomware attack, your data is targeted and encrypted by criminals.

2. But LTO tape encryption makes it almost impossible for any malicious actor to steal or manipulate your data.

3. And best of all, you hold all the keys and have complete control.