True Cost of **Ransomware** to Your Business

Technological advancements have led to an exponential growth in the rate of cybercrimes and will only continue to do so in the future.

Ransomware is one such a dangerous malware that infects computers and/or mobile devices and restricts access to files, often threatening to permanently destroy data unless a ransom payment is made.

DID YOU KNOW?

Ransomware is expected to hit a business every 11 seconds before the end of 2021!

Ransomware will magnify and represent a proportionately larger share of total cybercrime by 2021.

Ransomware Damage Costs

Ransomware damage costs are not limited to ransom pay outs but includes:

- Damage and destruction/loss of data
- Downtime, lost productivity
- Post-attack disruption to the normal course of business
- Forensic investigation, restoration and deletion of hostage data and systems
- Reputation loss, and employee training in direct response to the ransomware attacks

Some Important and Shocking Statistics:

- Global costs due to ransomware damage are projected to reach $20 billion by 2021 – this amounts to 57X more than it was in 2015.
- 91% of cyberattacks start with spear-phishing emails, which are often used by hackers to infect organizations with ransomware.
- According to an estimate by Cybersecurity Ventures, cybercrime will cost the world over $6 trillion annually by 2021, compared to $3 trillion in 2015.
- Organizations saw a record 225% increase in losses from ransomware attacks in 2020.
- 53% of businesses stated that their brand and reputation were damaged after a successful attack.
- Among the organizations that agreed to pay a ransom amount to recover their data, 46% reported that nearly all their data was corrupted in the process.
- 80% of the companies that chose to pay the ransom amount were victims of a second ransomware attack, often by the same group of perpetrators.
- Employees were laid off by 29% of the firms due to financial pressures following the attack.
- A shocking 26% of enterprises had to shut down operations permanently because of a ransomware attack.

The Way Forward

Since ransomware uses social engineering as its primary infection vector, it is essential to spread cybersecurity awareness among everyone in an organization.

This includes everyone from CIOs, CISOs, IT security teams, and employees.

Engaging and informative methods like phishing simulation programs and awareness programs can be used to heighten cybersecurity awareness in the organization.

Note: Cybersecurity awareness training is the most under spent sector of the cybersecurity industry, but it is the biggest hope for overcoming ransomware attacks.

Grow Your Business Securely with Indusface

Be proactive and secure your business to avoid paying millions of dollars in damages.

With Indusface WAF, which integrates web application scanning, pen testing, and virtual patching in a single security solution you can effectively detect and block malicious requests and traffic.

Contact us now to schedule 14 Days Free Trial.

indusface.com