HEALTHCARE

HOW RANSOMWARE THREATENS YOUR ORGANIZATION

Ransomware attacks are rapidly increasing in frequency and cost. Organizations victimized by ransomware attacks can lose access to their networks and data, incur steep financial losses, and suffer significant reputation damage.

COVID-19 PANDEMIC FUELS OUTBREAK OF RANSOMWARE

Attacks against healthcare organizations rose 350% between 2018-2019.

Ransomware damages rose 230%

- 2017: $5B
- 2019: $11.5B

HOW LONG CAN you afford to close your doors?

The average downtime from a ransomware attack is 9.6 days.

WHICH SECTORS are most at risk?

- SMBs: 60%
- Healthcare: 29%
- Government: 15%
- Professional Services: 14%
- Financial Institutions: 11%

Small entities, BIG CYBER RISKS

Ransomware preys on state, county and municipal governments with limited resources.

163+ ransomware attacks hit local & county governments in 2019.

59% increase in known attacks on local governments from 2018-2019.

104% increase in average ransom payment amounts.

HEALTHCARE IS A TOP TARGET

Attacks against healthcare organizations rose 230% between 2018-2019.

RANSOMWARE ATTACKS TO PROTECT YOUR BUSINESS AGAINST RANSOMWARE

1. Perform regular system backups
2. Train employees to avoid phishing and other scams
3. Require the use of a password manager
4. Subscribe to a dark web monitoring solution


SOURCES:
1. Dark Reading
2. Cybersecurity Ventures
3. Dark Reading
4. CIO Dive
5. Dark Reading
6. Dark Reading
7. Hashed Out News
8. Beckers Hospital Review