A CRASH COURSE ON SOLVING ONE OF YOUR MOST TERRIFYING SECURITY THREATS

WHAT TO EXPECT IN THE FUTURE?

RANSOMWARE WILL BECOME EVEN MORE TARGETED.
RANSOMWARE WILL BE EVEN HARDER TO DETECT
AND BETTER EQUIPPED TO PLOW THROUGH YOUR EXISTING PROTECTIONS.
RANSOMWARE WILL GO AFTER MOBILE AND INTERNET OF THINGS DEVICES MORE FREQUENTLY.

3 REASONS RANSOMWARE EXPLODED SO QUICKLY

1. Continued professionalization and organization of the cybercriminal underground.
2. Lower risk afforded by the rising popularity of anonymous cryptocurrency payment methods such as Bitcoins.
3. It works! Ransomware attacks now outnumber data breaches because they are easy to launch and victims are paying up.

YOUR ESSENTIAL CHECKLIST FOR RESISTANCE, RESCUE AND RECOVERY

BEFORE

TURN SECURITY AWARENESS INTO REPEATABLE PROCESSES:
Train your employees to stay on top of phishing attacks, and rehearse what to do if they receive suspicious emails and other messages.

DO THE BASICS:
Keep your systems, plug-ins and extensions up to date – and follow the principle of least privilege for your users.

IMPLEMENT TECHNOLOGY SAFEGUARDS:
Help stop infiltration to root out how and why attacks succeed, protect both personal and organizational assets together.

BACK UP YOUR SYSTEMS:
Backing up your sensitive information can be your most valuable defense against ransomware. Double-check their integrity and keep them in an off-site, secure location.

DURING & AFTER

GET OFFLINE:
If you’re hit with ransomware, disconnect the affected systems from the internet.

PRACTICE R&R:
Ensure you both reimage your machines and restore your data.

ASSESS YOUR LEGAL OBLIGATIONS:
If you notify customers about a ransomware attack, be sure to follow federal and state laws.

TRY TO AVOID PAYING:
Remember, even if you pay the ransom, there is no guarantee the attackers will release the decryption keys.

PERFORM FORENSICS:
Discover how the attack unfolded so measures can be taken to block the same type of attack in the future.

TECHNICAL BONUS TIP
Hit with ransomware but don’t know which computer is infected? On the encrypted file, go to “properties” to find out who the owner of the file is. This will help you track down the compromised machine.

Source:
[221x941]SOME ORGANIZATIONS FACE MULTIPLE RANSOMWARE INCIDENTS EACH WEEK.
AT LEAST ONE VICTIM HAS EXPERIENCED 21 ATTACKS IN THE PAST YEAR.
30% TO 40% OF BUSINESSES EXPERIENCED A RANSOMWARE ATTACK OVER THE PAST YEAR.

Note:
No industry or organization is immune from being targeted by a ransomware attack.

3 REASONS RANSOMWARE EXPLODED SO QUICKLY
1. Continued professionalization and organization of the cybercriminal underground.
2. Lower risk afforded by the rising popularity of anonymous cryptocurrency payment methods such as Bitcoins.
3. It works! Ransomware attacks now outnumber data breaches because they are easy to launch and victims are paying up.

PAY NOW