groupsense

RANSOMWARE LESSONS FROM THE TRENCHES

From renowned ransomware negotiator, Kurtis Minder

GroupSense is a digital risk protection services company and does some of the largest negotiations for ransomware. Financial services is 300x more likely to be a victim of a cyberattack compared than any other industry.

LESSONS FROM THE TRENCHES

12 lessons from renowned ransomware negotiator and CEO of GroupSense, Kurtis Minder, on what happens after a ransomware attack.

Do Not Panic
You have options. This is recoverable. Revert to your plan and execute.

Do Not Engage
Don't let anyone go to the site / respond. It can start a timer. Tone, language, style, and content can significantly impact odds and costs negatively.

Don't Shut Down
Don't shut down machines, this can cause file corruption, and hinders the incident response process.

Do Not Bury Your Head
Having backups and restoring doesn't mean this is over. There are many other things to consider.

Engage Legal Counsel
It is likely you are subject to breach disclosure laws - bring legal help to determine your obligations.

Engage PR Support
You will have to notify impacted constituents. Do this carefully and with professional guidance.

Engage IR
Bring in incident response assistance to understand the scope of the attack and to ensure the threat actors no longer have access.

DIGITAL PANDEMIC

The value of ransom demands has gone up, with some demands exceedingly well over $1 million. - Cybersecurity & Infrastructure Security Agency, 2021

The total ransomware costs are projected to exceed $20 billion in 2021. - Cybercrime Magazine, 2019

Financial Services was the top targeted sector in 2019 and 2020. - IBM, 2020

On average, ransomware attacks cause 15 business days of downtime. Due to this inactivity, businesses lost around $8,500 an hour. - Health IT Security, 2020

Sector increased 238% globally from the beginning of February 2020 to the end of April 2020. - Vmware, 2020

Contact Insurance
Your insurer may have requirements dictating how the response is carried out. Engage them early.

Bring in a Professional Responder
Bring in a professional that has firsthand experience with the entire ransomware process.

Consider Sanctions
Your country may have rules about which entities you can transact with. Responders can help you avoid penalties.

Notify Law Enforcement
It is best practice to make local law enforcement aware of the situation.

Monitor
It is likely the threat actor took a significant amount of data. Monitor just in case it surfaces elsewhere.

TIPS ON HOW TO PROTECT YOURSELF

GroupSense's team of experienced negotiators developed cybersecurity tips to help reduce your risk. Below is a sample, for the full list, please visit https://www.groupsense.io/tips-to-better-protect-your-data-from-ransomware

Password Policy & Email Security/ Email Policy
Have a strong policy about using corporate email for personal use. Restrict access to personal mail on company assets. Maintain and publish a password policy for your organization. The policy should illustrate the importance of password security and credential use in the organization.

Use a password manager
Use an enterprise-friendly password manager and require employees to use this as part of the security program.

Enable Multi-Factor Authentication Everywhere Possible
Enable the 2FA or MFA capability on everything used in the business. This includes email, network access, remote access, and any web-based applications.

Patch

Backups
Keep at least one manual backup of your data offsite in a secure location.

Secure Remote Access
If remote access is required, use a zero-trust access method or a VPN. Use two-factor authentication.

GroupSense's Ransomware Response Readiness Subscription (R^3S) gives organizations the best chance to survive and recover. Receive the intelligence you need to take action quickly and decisively. If you'd like to talk to an analyst, contact us at 1-877-469-7226, or email sales@groupsense.io

ABOUT GROUPSENSE

GroupSense is a digital risk protection services company that delivers customer-specific intelligence that dramatically improves enterprise cybersecurity and fraud-management operations. Unlike generic cyber-intelligence vendors, GroupSense uses a combination of automated and human reconnaissance to create finished intelligence that maps to each customer's specific digital business footprint and risk profile. This enables customers to immediately use GroupSense's intelligence to reduce enterprise risk, without requiring any additional processing or management by overstretched security and fraud-prevention teams.

GroupSense is based in Arlington, Va., with a growing customer base that includes large enterprises, state and municipal governments, law enforcement agencies and more.

Find out how GroupSense can help your organization at www.groupsense.io