Cybersecurity Discussion

Brought to you by: level❷

"Taking your business to the next level"

Presenters

Daniel Stanton

President – Chief Security Officer

Jonathan Madelmont

VP Cloud & Managed Security

Ransomware

- Demand large payments to decrypt stolen data or to prevent it from being leaked online.

  - Payment: Cryptocurrency

- The U.S. government recommends that ransomware victims **NOT** pay their attackers. *Would you not pay your ransom if it was your business?

- Increasing number of attacks prey on small- to medium-sized entities

Ransomware cont.

- **Top Entry Points – Attack Vectors**
  - Email (recent leader shift)
    - Phishing - Malspam
    - Links
    - Spoofing – Display Name, Gift Cards
  - Remote Desktop Protocol
  - Software Vulnerability
    - Updates, Patching, Zero-day
  - Stolen or Weak Credentials
    - Unencrypted communication
- **Trickbot and EMOTET**
  - Worming Capabilities – Lateral Movement
  - Networked Devices

Recent Events

Colonial Pipeline

May 7

- **$4.4 million**
- Control-room computer
- Unknown severity – Immediate shutdown for a week
- One password was breached – No 2 Factor!

JBS (World's largest meat processor)

May 30

- **$11 million**
- Shutdown for at least a day
- Spends more than **200m** on IT and employs more than **850** tech specialists
- Cybercriminal group: "one of the most specialized and sophisticated"
- Good backup is necessary!

Recent Events cont.

Washington DC Police Department

April 26

- Data Hostage – Released to the dark web.
- Wanted **$4 million** not to release the files, but was only offered $100,000.
- Officer professional and personal info – background checks, evaluations finances, etc.

Insurance

- Europe's Top Five Insurer "**AXA**"

- France: Deny payment of ransomware

- Only the U.S. surpassed France last year in damage from ransomware to business, hospitals, schools and local governments, estimating France's related overall losses at more than **$5.5 billion**

- The average recover time from a ransomware attack is three weeks.

- Review your Cyber Security Insurance!

Cybersecurity: A Layered Approach

Next Gen Firewall	Web Filtering	Next-Gen Endpoint Protection	Password Manager
Intrusion Prevention System (IPS)	Category-based content	Windows and Mac Operating Systems	Store and Manage Passwords
Protects against known threats and zero-day attacks including malware and underlying vulnerabilities	Block malware, phishing, command and control callbacks, crypto-mining, botnet	AI approach, predicting & protecting against known and unknown malware, fileless attacks, and zero-day payload execution	Share Multi-Factor Authentication Tokens
Policies and Ports	Reporting	Alerting, behavioral analysis, and patch management	Sharing – User and Group Permissions
Client SSL VPN		Control use of USB storage devices	Detect weak and compromised passwords
Application Control			

level2

Multi-Factor Authentication	Users: Security Awareness Training	Zero Trust Network Access ZTNA	Backups
Two or more verification factors	Simulated Email Attacks	Least Privilege – Folders, Files, Network, Applications	Automated Local and Cloud
Mobile App, Hardware Key, SMS, Call, Email, Biometrics	Scheduled Training and Reports	Device Health – Software, Updates	Offsite and Offline Storage
Notification, Rotating One-time Passwords (OTP), Certificates	Automatic enrollment, notification, deadlines	"New" Remote Access and VPN	Recycle Bin - Rogue Admin, Accidental
Conditional Access – Location (Country to IP address), Device, Hours			Protection against Ransomware

Level 2 Designs

- We are not just your IT service provider, we are your strategic partner.

- Our Customers Trust Us Because We:
  - Define then align goals for IT along with the business
  - Leverage the latest technology to drive efficiency, profitability, and growth
  - Continually assess and improve infrastructure
  - Focus on Business Security

- Partners:

Clients

Questions
&
Answers