CLOUD SECURITY AND RANSOMWARE

POTENTIAL RISKS AND MITIGATION STRATEGIES

David Cole

SysAudits.com LLC

RANSOMWARE STATISTICS

- **In 2020 - a total of 304 million ransomware attacks worldwide.**
- **A 62 percent increase from 2019**
- **Second highest since 2016**
- **Stats are only what was reported – probably double the number!**

- **Recent ransomware attacks have targeted a wide range of high-profile organizations and companies**
- **Colonial Pipeline - JBS Food -ACER -Kia Motors**
- **Police Departments -Healthcare -Pharmaceuticals**

WHAT IS RANSOMWARE?

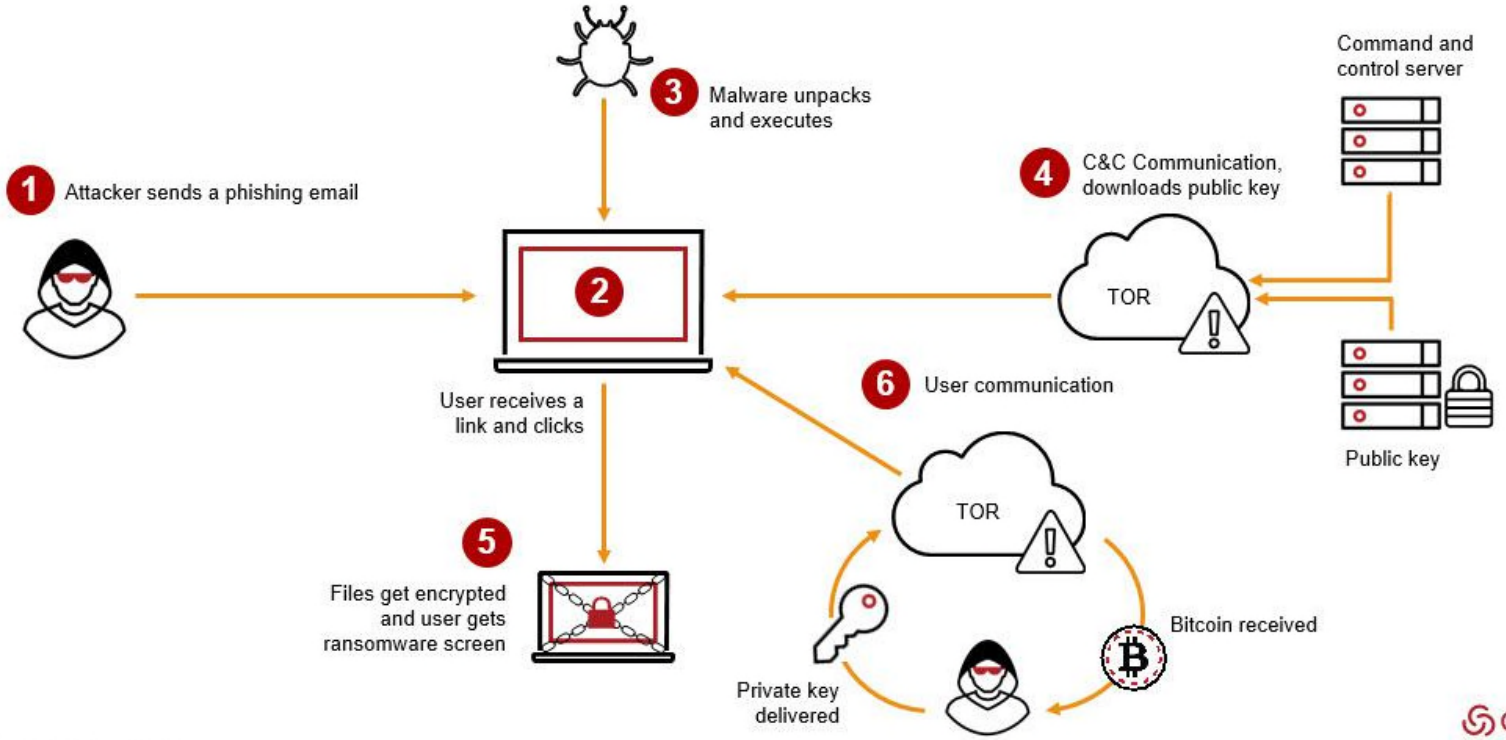
- **Ransomware is a form of malware.**
- **Designed to encrypt files on a device, network, or storage**
- **Encryption will render files and the systems inaccessible and unusable.**
- **Malicious actors then demand ransom in exchange for decryption.**
- **Bitcoin is the currency demanded.**

RANSOMWARE STAGES
(EXABEAM – THREAT RESEARCH REPORT – ANATOMY OF A RANSOMWARE ATTACK

The main stages of the Ransomware Kill Chain are as follows:

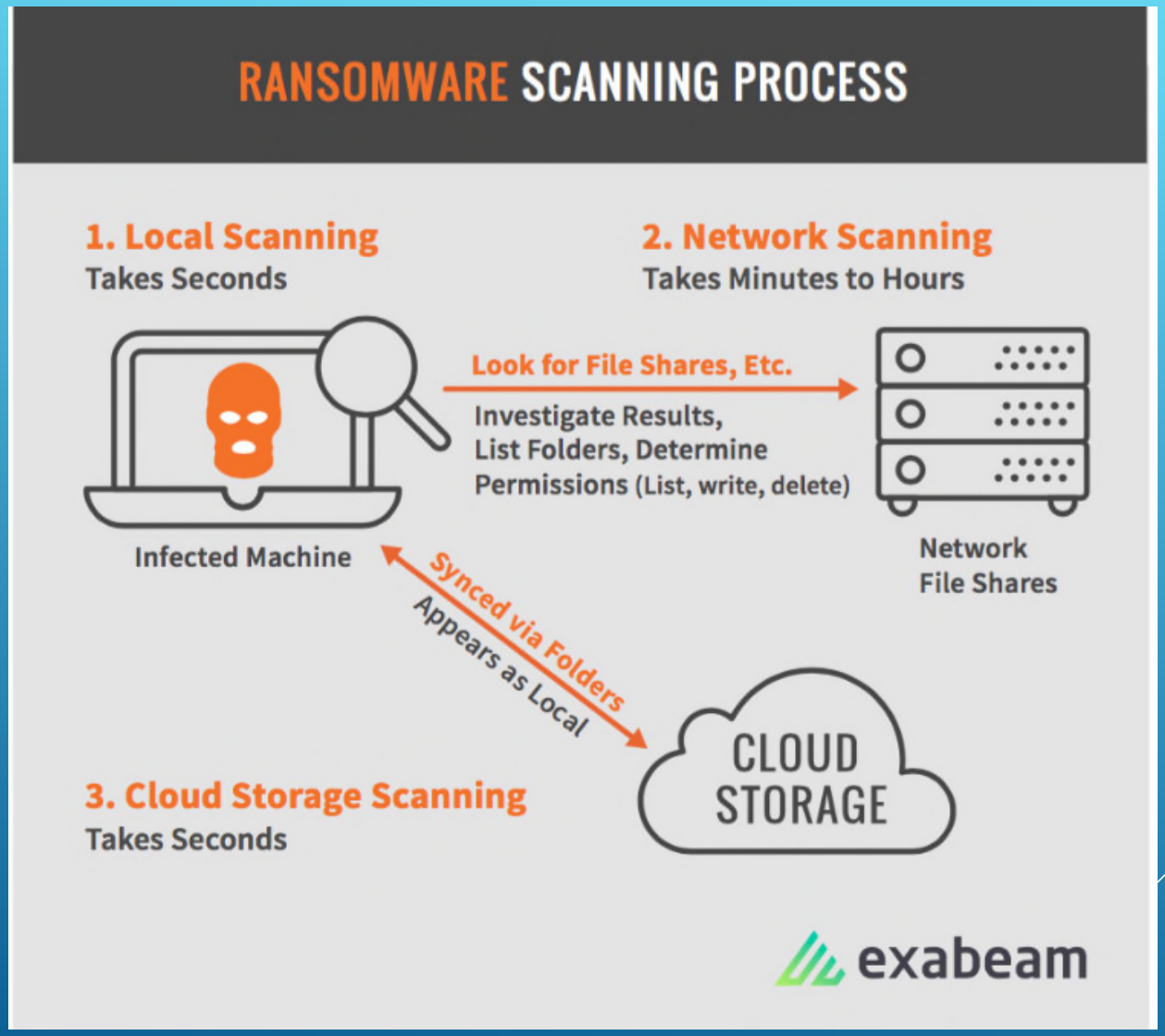
1. **Distribution campaign** – attackers use techniques like social engineering and weaponized websites to trick or force users to download a dropper which kicks off the infection
2. **Malicious code infection** – the dropper downloads an executable which installs the ransomware itself
3. **Malicious payload staging** – the ransomware sets up, embeds itself in a system, and establishes persistency to exist beyond a reboot
4. **Scanning** – the ransomware searches for content to encrypt, both on the local computer and the network accessible resources
5. **Encryption** – the discovered files are encrypted
6. **Payday** – a ransom note is generated, shown to the victim, and the hacker waits to collect on the ransom

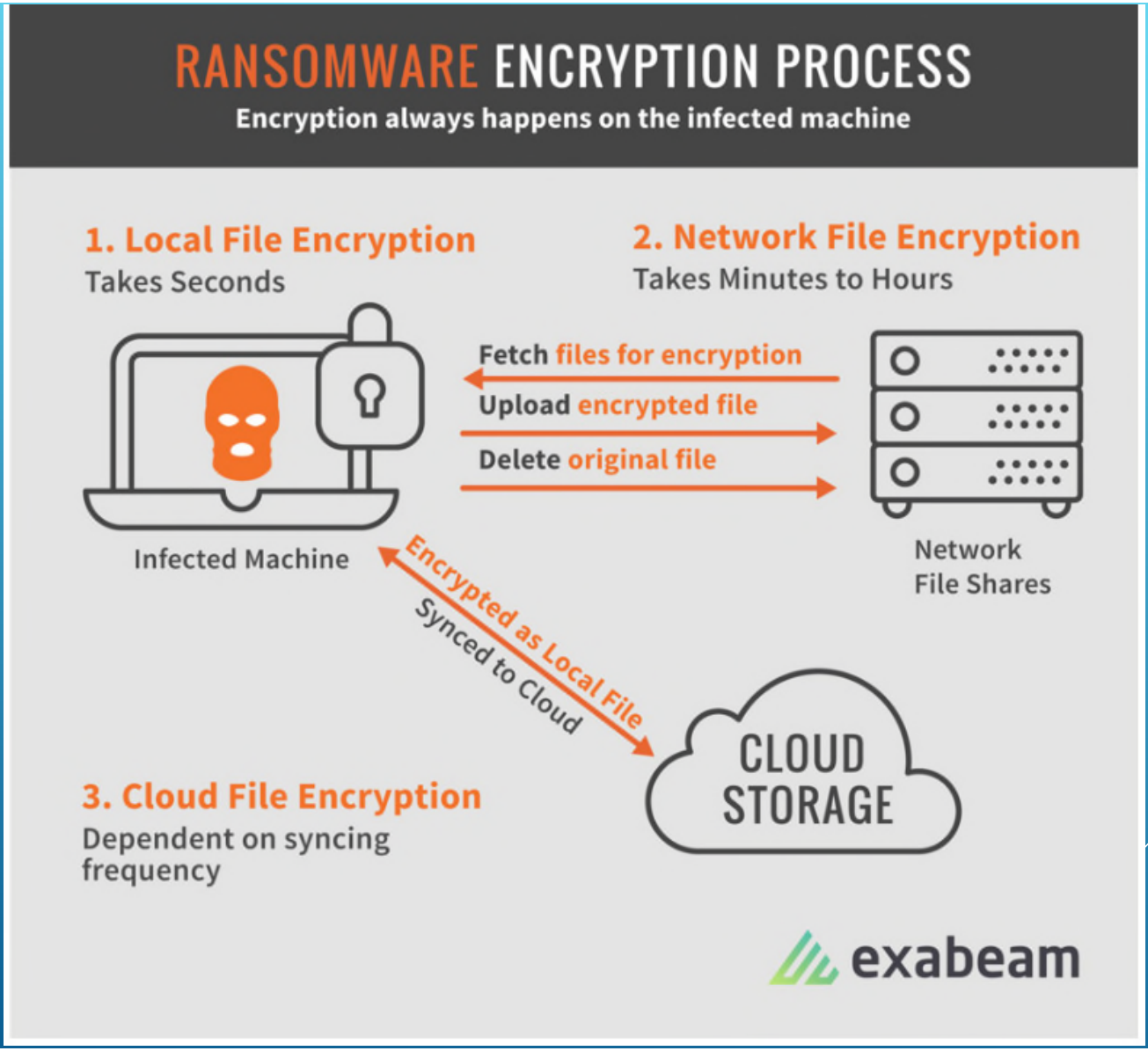
The Anatomy of a Ransomware Attack



Centrify
ZERO TRUST PRIVILEGE

Source: Centrify - Privileged Access Management


RANSOMWARE SCANNING PROCESS
1. Local Scanning
Takes Seconds
2. Network Scanning
Takes Minutes to Hours
Look for File Shares, Etc.
Investigate Results,
List Folders, Determine
Permissions (List, write, delete)
Infected Machine
Network
File Shares
Synced via Folders
Appears as Local
CLOUD
STORAGE
3. Cloud Storage Scanning
Takes Seconds
exabeam


RANSOMWARE ENCRYPTION PROCESS
Encryption always happens on the infected machine
1. Local File Encryption
Takes Seconds
2. Network File Encryption
Takes Minutes to Hours
Fetch files for encryption
Upload encrypted file
Delete original file
Infected Machine
Network
File Shares
Encrypted as Local File
Synced to Cloud
CLOUD
STORAGE
3. Cloud File Encryption
Dependent on syncing
frequency
exabeam

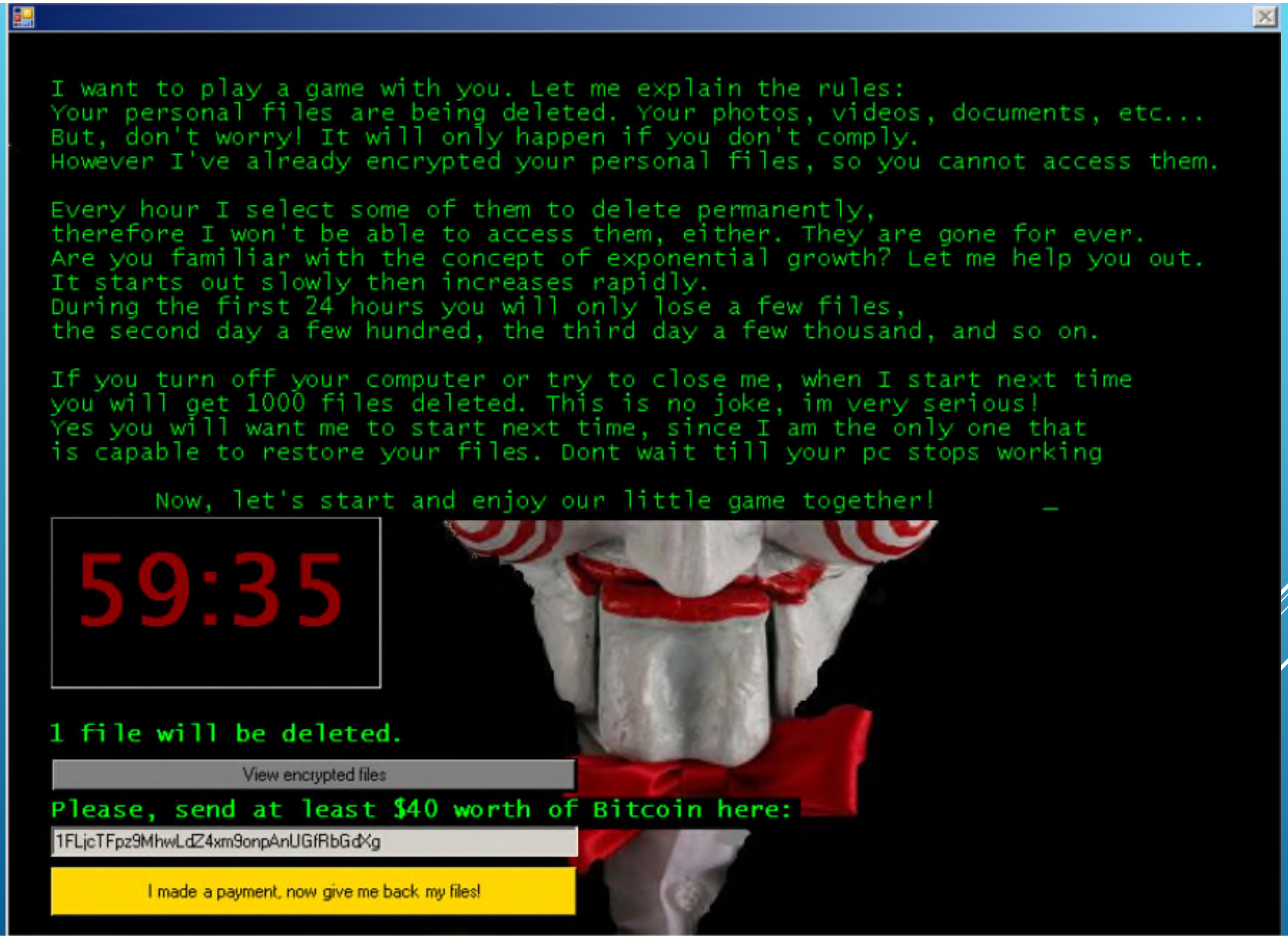
RANSOMWARE INDICATORS

What are the indicators of a ransomware attack?

- **Your locked out!**
- **May notice odd file extensions, files with appended extensions .doc.xzt**
-

Intimidating messages:

- **"Your computer has been infected with a virus. Click here to resolve the issue."**
- **"Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a $100 fine."**
- **"All files on your computer have been encrypted. You must pay this ransom within 72 hours to regain access to your data."**


I want to play a game with you. Let me explain the rules:
Your personal files are being deleted. Your photos, videos, documents, etc...
But, don't worry! It will only happen if you don't comply.
However I've already encrypted your personal files, so you cannot access them.
Every hour I select some of them to delete permanently,
therefore I won't be able to access them, either. They are gone for ever.
Are you familiar with the concept of exponential growth? Let me help you out.
It starts out slowly then increases rapidly.
During the first 24 hours you will only lose a few files,
the second day a few hundred, the third day a few thousand, and so on.
If you turn off your computer or try to close me, when I start next time
you will get 1000 files deleted. This is no joke, im very serious!
Yes you will want me to start next time, since I am the only one that
is capable to restore your files. Dont wait till your pc stops working
Now, let's start and enjoy our little game together!
59:35
1 file will be deleted.
View encrypted files
Please, send at least $40 worth of Bitcoin here:
1FLjcTFpz9MhwLdZ4xm9onpAnUGfRbGdXg
I made a payment, now give me back my files!

NEGATIVE IMPACTS OF RANSOMWARE

Ransomware targets businesses, governments, and home users

Ransomware consequences, include:

- **temporary or permanent loss of sensitive or proprietary information**
- **disruption to regular operations**
- **financial losses incurred to restore systems and files,**
- **potential harm to an organization's reputation, and**
- **significant downstream impact to business partner, third-party, and client costs**

  (any interconnected systems are at risk of lateral movement into their environment)

NEGATIVE IMPACTS OF RANSOMWARE

- **Paying the ransom does not guarantee the encrypted files will be released**
- **This only guarantees that the malicious actors receive the ransom funds**

- **Decrypting files does not mean the malware infection itself has been removed**

- **In all likelihood, there will be an attempt to extort money funds**

AUDIT RISK PLANNING
RANSOMWARE PREVENTION AND MITIGATION

Many Potential Audit Objectives tied to IT security and ransomware risk management

The following activities and processes are applicable to an on-prem, cloud deployment, or mixed environment

- **Effective Identity Access Management**
- **Effective Backup Procedures**
- **Vulnerability Management - vulnerability, compliance, active phishing**
- **Secure Configuration Management**

AUDIT RISK PLANNING
RANSOMWARE PREVENTION AND MITIGATION

Many Potential Audit Objectives tied to IT security and ransomware risk management

- **Patching and Updates**
- **Incident Response Management**
- **Security Assessments**
- **Security awareness and training**
- **Least privilege across all infrastructure**
- **Segregation of duties**
- **Separate accounts and account re-certification**

RANSOMWARE PREVENTION AND MITIGATION – IDENTITY ACCESS MANAGEMENT - EXAMPLE

- **Employ multi factor authentication for all services to the extent possible**
- **Remote access, webmail, VPN, cloud provisioning, and accounts that access critical systems**
- **Very important for activities and processes that use privileged accounts (administration at the OS, DB, NW, FW, Apps)**
- **Domain admins, admins that control pushing patching and updates, agent deployments**

RANSOMWARE PREVENTION AND MITIGATION – IDENTITY ACCESS MANAGEMENT - EXAMPLE

Password Management

- **Still need to use strong passwords settings (complexity, length, change periodically**

- **Use strong passwords and do not reuse passwords for multiple accounts.**
  - **Change default passwords**
  - **Enforce account lockouts after a specified number of login attempts.**
  - **Password managers can help you develop and manage secure passwords**

RANSOMWARE PREVENTION AND MITIGATION – IDENTITY ACCESS MANAGEMENT – EXAMPLE

- **Apply the principle of least privilege to all systems and services**
- **Users only have the access needed to perform their jobs**

Hackers/Threat Actors
- **seek out privileged accounts to leverage to execute ransomware attacks**

Least privilege principles include:
  - **Restrict user permissions to install and run software applications – no local admin!**
  - **Restrict remote access capability**
  - **Admins also have minimal privileged access**
  - **Review all accounts: users, admins, dba, application, and system/service**
    - **Its painful, but if an inventory of accounts + reviews with restrictions performed vs. paying out millions, can make a cost/benefit decision**

RANSOMWARE PREVENTION AND MITIGATION – IDENTITY ACCESS MANAGEMENT – EXAMPLE

- **Remove unnecessary accounts and groups and restrict root/domain admin access. Apply access control best practices such as:**
  - **Control and limit local administration**
  - **Leverage Protected Users Active Directory group in Windows domains to further secure privileged user accounts against pass-the-hash attacks**
  - **Audit user accounts regularly, particularly Remote Monitoring and Management accounts that are publicly or internally accessible**

RANSOMWARE PREVENTION AND MITIGATION – DATA BACKUP - EXAMPLE

Critical to maintain offline, encrypted data backups
Regularly test backups – DR tests to an alternate site – limits potential risk of re-infestation

Critical backups of data should include:

- **Regularly update "gold images" of critical systems**
- **Pre-configured OS images**
- **Inventory of critical software, versions, vendor POCs, installation priorities**
- **Virtual system snapshots if hosts are VMs**

- **Applicable source code or executables should be available (stored with backups, escrowed, license agreement to obtain, etc.).**

- **Ops Insight: May be more effective to rebuild from system images**
- **However, may have issues if rebuilding on different hardware or platforms**
- **Access to safe software, gold images, virtual snapshots**

RANSOMWARE PREVENTION AND MITIGATION – PATCHING AND UPDATING - EXAMPLE

- **Limit Attack Surface: Conduct regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices**
- **Strict patching and software updating – OS, DB, NW devices, FW, Apps with latest available versions**
- **Process for third-party software updating – Adobe, etc.**
- **Periodic recertification of ACL's at routers, firewalls, IDS, IPS, Hosts**

RANSOMWARE PREVENTION AND MITIGATION – SECURE CONFIGURATION MANAGEMENT

- **Ensure devices are properly configured and that security features are enabled**
- **disable unnecessary ports and services not used for a business purpose - painful**
- **limit and restrict use of remote desktop protocol (RDP) and other remote desktop services**
  - **Hackers/threat actors gain initial access to a network through exposed and poorly secured remote services, and later propagate ransomware.**
- **Audit and log systems using RDP, enforce account lockouts after failed attempts, apply MFA, and log RDP login attempts**

RANSOMWARE PREVENTION AND MITIGATION – INCIDENT RESPONSE PLAN - EXAMPLE

- **Cyber Incident Handling Plan: Create, maintain, and exercise a incident response plan**
  - **Include communications plan with notification procedures for a ransomware incident**

- **A cyber incident response plan with procedures to address the following:**
  - **Isolate the infected computer immediately**
  - **Isolate or power-off affected devices**
  - **Immediately secure backup data or systems**
  - **Contact law enforcement**
  - **Securing partial portions of the ransomed data that might exist**
  - **Changing all online account and network passwords**
  - **Deleting Registry values and files**

CLOSING THOUGHTS AND POINTS

Ransomware is here to stay

Controls for IT operations and IT security practices for on-prem, cloud, or mixed environments are still the same as they were before the rise in ransomware albeit some unique risks

Under an Audit: Lots of opportunities to support mitigating ransomware attack risks by:

- **Practice good cyber hygiene**
- **Know your system security risks and have a plan to mitigate**
- **Test, update, and review recovery procedures**
- **Develop and review Incident Response containment strategies**
- **Ensure SIEM is receiving security relevant logs and a log review process is in place**

QUESTIONS?

Survey: Do you see a value in a ransomware IT audit seminar?

REFERENCES

1. https://www.cisa.gov/cybersecurity-training-exercises
2. https://www.cisa.gov/stopransomware
3. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
4. https://www.cisa.gov/stopransomware/sector-risk-management-agencies
5. https://www.cisa.gov/stopransomware/ransomware-101
6. https://csrc.nist.gov/projects/ransomware-protection-and-response
7. https://www.publicpower. org/system/files/documents/Public-Power-Cyber-Incident-ResponsePlaybook.pdf