HITRUST WEBINAR:

Ransomware and Mitigating the Impact of an Attack

Thursday, September 9, 2021

12:00-1:00pm CDT

HITRUST®

Presented By:

LESLIE WEINSTEIN
Solutions Director
HITRUST

Agenda:

- Ransomware defined
- How ransomware is delivered and what happens when you become a victim
- What to do if you become a victim
- Strategies for preventing an attack
- Strategies for mitigating an attack

SECTION 1

Ransomware Defined

What is Ransomware?

"Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption."

Source: https://www.cisa.gov/stopransomware

Who is CISA?

- The Cybersecurity and Infrastructure Security Agency (CISA) is part of the Department of Homeland Security (DHS)
- CISA serves as the Nation's risk advisor and builds the national capacity to defend against cyber attacks
- Works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies

Source: https://www.cisa.gov/stopransomware

SECTION 2

How Ransomware is Delivered and What Happens When You Become a Victim

Ransomware Delivery Mechanisms

- Email Phishing Campaigns
  - Could be a targeted or generic broad-based attack
  - Uses social engineering
- Remote Desktop Protocol (RDP) Vulnerabilities
  - RDP allows users to control a remote machine from a local machine
  - Brute-force attacks and purchased credentials used to access RDP
- Software Vulnerabilities
  - Zero-day and known (but unpatched) vulnerabilities

Source: https://www.cisa.gov/sites/default/files/2021-01/NCIJTF%20Ransomware_Fact_Sheet.pdf

What happens when you become a victim?

- A U.S. county was infected by Ryuk, taking almost all of the county's systems offline. The county had backup servers, but
- A U.S. county's computer systems were infected by Ryuk. The attackers demanded over $1.2 million in Bitcoin for a decryption key. Officials decided to rebuild their systems
- A U.S. city's systems were infected by Robbinhood with a ransom demand of 13 Bitcoins ($76,000). The attackers entered the network through old, out-of-date hardware and software. The ransom was not paid, but service restoration was estimated to cost over $9 million.

SECTION 3

What to Do if You Become a Victim

What to Do When Ransomware Hits

Detect and Analyze:

1) Determine which systems were impacted, and immediately isolate them
2) Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection
3) Triage impacted systems for restoration and recovery
4) Consult with your incident response team to develop and document an initial understanding of what has occurred based on initial analysis
5) Engage your internal and external teams and stakeholders with an understanding of what they can provide to help you mitigate, respond to, and recover from the incident
6) Report incident as required (HIPAA, DFARS, etc.)

Source: https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

If Recovery isn't Possible…

- Take a system image and memory capture of a sample of affected devices
  - Workstations and Servers
- Collect any relevant logs as well as samples of any "precursor" malware binaries and associated observables or indicators of compromise
  - Suspected command and control IP addresses, suspicious registry entries, or other relevant files detected
- Take care to preserve evidence that is highly volatile in nature - or limited in retention - to prevent loss or tampering
  - System memory, Windows Security logs, data in firewall log buffers
- Consult federal law enforcement regarding possible decryptors available, as security researchers have already broken the encryption algorithms for some ransomware variants

SECTION 4

How to Mitigate the Impact of an Attack

HITRUST CSF Threat Catalogue™

The HITRUST CSF Threat Catalogue provides a list of 'reasonably anticipated' threats, enumerated at a level commensurate with HITRUST CSF control requirements, and maps these threats to HITRUST CSF v9.4.x controls at a level commensurate with their specification (i.e., description of the control).

						Type	Logical Threats	Logical Threats	Logical Threats
						Category	Intentional	Intentional	Intentional
CSF v9.x						Sub-category	Conflict	Conflict	Conflict
						ID	LIC1	LIC2	LIC3
CONTROL CATEGORY	CONTROL OBJECTIVE NUMBER	CONTROL OBJECTIVE NAME	CONTROL OBJECTIVE	CONTROL NUMBER	CONTROL NAME	CONTROL SPECIFICATION	Sabotage	Terrorism	Vandalism
Information Security Management Program	**0.01**	**Information Security Management Program**	To implement and manage an Information Security Management Program.	0.a	Information Security Management Program	An Information Security Management Program (ISMP) shall be defined in terms of the characteristics of the business, and established and managed including monitoring, maintenance and improvement.	X	X	X
	1.01	**Business Requirements for Access Control**	Access to information and information processing facilities is limited.	01.a	Access Control	Access control requirements are formally established, documented and reviewed based on business and information security requirements.	X	X	X
	1.02		User access is authorized and unauthorized access to systems	01.b	User Registration and De-Registration	A formal user registration and de-registration process is used to verify a user's identity and enable assignment of access rights.	X	X	X
				01.c	Management of Privileged Access Rights	The allocation and use of privileged access rights are restricted and controlled.	X	X	X

HITRUST CSF Practices to Prevent a Ransomware Attack

DOMAIN	CONTROL NAME	CONTROL SPECIFICATION
Information Security Management Program	Information Security Management Program	An Information Security Management Program (ISMP) shall be defined in terms of the characteristics of the business, and established and managed including monitoring, maintenance and improvement.
Asset Management	Inventory of Assets	Assets associated with information and information processing facilities are identified and an inventory of these assets are drawn up and maintained.
	Ownership of Assets	Assets maintained in the inventory are owned by an individual or a designated part of the organization.
	Acceptable Use of Assets	Rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented.
	Classification Guidelines	Information shall be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.

HITRUST CSF Practices to Prevent a Ransomware Attack

DOMAIN	CONTROL NAME	CONTROL SPECIFICATION
Access Control	Access Control	Access control requirements are formally established, documented and reviewed based on business and information security requirements.
	User Registration and De-Registration	A formal user registration and de-registration process is used to verify a user's identity and enable assignment of access rights.
	Management of Privileged Access Rights	The allocation and use of privileged access rights are restricted and controlled.
	User Password Management	Passwords shall be controlled through a formal management process.
	Review of User Access Rights	Access rights shall be regularly reviewed by management via a formal documented process.
	Policy on the Use of Network Services	Users are only provided with access to the network and network services that they have been specifically authorized to use.
	User Authentication for External Connections	Appropriate authentication methods shall be used to control access by remote users.
	Equipment Identification in Networks	Automatic equipment identification shall be used as a means to authenticate connections from specific locations and equipment.
	Segregation in Networks	Groups of information services, users and information systems are segregated on networks.
	Network Connection Control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted.
	Network Routing Control	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
	Secure Log-On Procedures	Access to operating systems shall be controlled by a secure log-on procedure.
	Password Management System	Password management systems are interactive and ensure quality passwords.
	Use of System Utilities	The use of utility programs that might be capable of overriding system and application controls are restricted and tightly controlled.
	Limitation of Connection Time	Restrictions on connection times shall be used to provide additional security for high-risk applications.
	Sensitive System Isolation	Sensitive systems shall have a dedicated and isolated computing environment.

HITRUST CSF Practices to Prevent a Ransomware Attack

DOMAIN	CONTROL NAME	CONTROL SPECIFICATION
Human Resources	Information Security Awareness, Education and Training	Employees of the organization and, where relevant, contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.
	Removal of Access Rights	The access rights of all employees and external party users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change.
Security Policy	Policies for Information Security	Policies for information security are approved by management, published and communicated to employees and relevant external parties.
	Review of the Policies for Information Security	Policies for information security are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
Organization of Information Security	Identification of Risks Related to External Parties	The risks to the organization's information and information assets from business processes involving external parties shall be identified, and appropriate controls implemented before granting access.
	Addressing Security When Dealing with Customers	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
	Addressing Security Within Supplier Agreements	All relevant information security requirements are established and agreed with each supplier that may access, process, store, or communicate the organization's information, or provide IT infrastructure components for such use.
Compliance	Prevention of Misuse of Information Assets	Users shall be deterred from using information assets for unauthorized purposes.
	Technical Compliance Checking	Information systems are regularly reviewed for compliance with the organization's information security policies and standards.

HITRUST CSF Practices to Prevent a Ransomware Attack

DOMAIN	CONTROL NAME	CONTROL SPECIFICATION
Communications and Operations Management	Service Delivery	Supplier service delivery is regularly monitored, reviewed and audited.
	Monitoring and Review of Supplier Services	Supplier service delivery is regularly monitored, reviewed and audited.
	Managing Changes to Supplier Services	Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, are managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.
	Controls Against Malicious Code	Detection, prevention, and recovery controls shall be implemented to protect against malicious code, and appropriate user awareness procedures on malicious code shall be provided.
	Controls Against Mobile Code	Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy. All unauthorized mobile code shall be prevented from executing.
	Network Controls	Networks are managed and controlled to protect information in systems and applications.

HITRUST CSF Practices to Prevent a Ransomware Attack

DOMAIN	CONTROL NAME	CONTROL SPECIFICATION
Communications and Operations Management (Continued)	Security of Network Services	Security mechanisms, service levels and management requirements of all network services are identified and included in network services agreements, whether these services are provided in-house or outsourced.
	Information Handling Procedures	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse
	Security of System Documentation	System documentation is protected against unauthorized access.
	Audit Logging	Audit logs recording user activities, exceptions, faults and information security events are produced, kept and regularly reviewed.
	Monitoring System Use	Procedures for monitoring use of information processing systems and facilities shall be established to check for use and effectiveness of implemented controls. The results of the monitoring activities shall be reviewed regularly.
	Protection of Log Information	Logging facilities and log information shall be protected against tampering and unauthorized access.
	Administrator and Operator Logs	System administrator and system operator activities are logged and the logs protected and regularly reviewed.
	Fault Logging	Faults shall be logged, analyzed, and appropriate remediation action taken.
	Clock Synchronization	The clocks of all relevant information processing systems within an organization or security domain are synchronized to a single reference time source.

HITRUST CSF Practices to Prevent a Ransomware Attack

DOMAIN	CONTROL NAME	CONTROL SPECIFICATION
System Act., Dev., & Maintenance.	Use of Cryptographic Controls	Requirements on the use of cryptographic controls for information protection are formally developed and implemented.
	Key Management	Requirements for the use, protection and lifetime of cryptographic keys is developed and implemented through their whole lifecycle.
	Outsourced Software Development	The activity of out- sourced system development is supervised and monitored.
	Management of Technical Vulnerabilities	Information about technical vulnerabilities of information systems being used are obtained in a timely fashion, the organization's exposure to such vulnerabilities are evaluated, and appropriate measures are taken to address the associated risk.

SECTION 5

Mitigating the Impact of an Attack

How to Mitigate Impact of Ransomware with the HITRUST CSF

DOMAIN	CONTROL NAME	CONTROL SPECIFICATION
Communications and Operations Management	Information Backup	Backup copies of information, software and system images are taken and tested regularly in accordance with an agreed backup policy.
Information Security Incident Management	Reporting Information Security Events	Information security events are reported through appropriate channels as quickly as possible.
	Incident Management Program	Management establishes a quick, effective and orderly response to information security incidents.
Business Continuity Management	Implementing Information Security Continuity	The required level of continuity for information security is established, implemented, and maintained during an adverse situation.
	Testing, Maintaining and Re-Assessing Business Continuity Plans	Business continuity plans shall be tested and updated regularly, at a minimum annually, to ensure that they are up to date and effective.

Be Prepared

- Maintain offline, encrypted backups of data and regularly test your backups
  - Maintain regularly updated “gold images” of critical systems in the event they need to be rebuilt. This entails maintaining image “templates” that include a preconfigured operating system (OS) and associated software applications that can be quickly deployed to rebuild a system, such as a virtual machine or server
- Create, maintain, and exercise a basic cyber incident response plan and an associated communications plan that includes response and notification procedures for a ransomware incident.

Be Prepared

- Develop and regularly update a comprehensive network diagram that describes systems and data flows within your organization's network
  - This can help incident responders understand where to focus their efforts
- Employ logical or physical means of network segmentation to separate various business unit or departmental IT resources within your organization as well as to maintain separation between IT and operational technology.
- Ensure your organization has a comprehensive asset management approach
  - Understand and inventory your organization's IT assets, both logical (e.g., data, software) and physical (e.g., hardware)

Q&A Session

THANK YOU FOR ATTENDING

For additional HITRUST resources, please visit:

HITRUSTAlliance.net or our Download Center

HITRUST®