M T W T F S S

Page No.: YOUVA

Date:

Cyber Security Breach Case Studies

W1

14/10/2022

⇒ Incident management response

↳ Establishing an incident response capability should include the following:

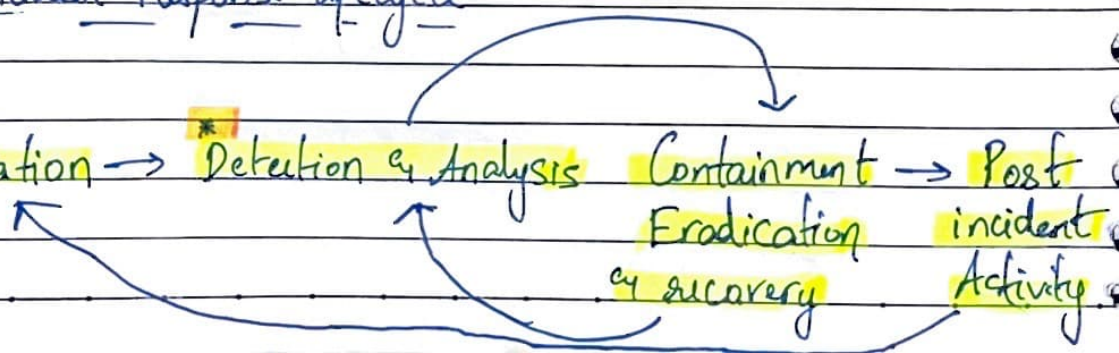
- establish a formal incident response capability
- create incident response policy
- Develop an incident response plan based on incident response policy
- develop incident response procedures
- Establish policies and procedures regarding incident-related information sharing
- Consider relevant factors when selecting incident response team model.

↳ Incident response team structure

1) Team model
2) Team model selection
3) Incident response personnel
4) Incident response team services

↳ NIST incident Response lifecycle

* identifying incident precursors and indicators



⇒ Virtual lab - Resilient

↳ How resilient can be used for your organization ?

- Insight into threats and risks through metrics
- Prevention through awareness and reporting
- Detect issues and round-the-clock management
- Respond to incident by applying best practices and ensure documentation using change management
- Recovery by enhancing prouses we have in place through incident review.

IRIS

⇒ Cyberattack frameworks

countermeasure : Build a threat profile of adversarial actors who are likely to target company

1) preparation framework
- conduct external recon
- Align tactics, techniques and procedures to target TTPs
- prepare malware and software tools
- prepare attack infrastructure

countermeasure : implement strong endpoint detection and mitigation strategies.

2) Launch and execute attack
- Access environment
- execute initial compromise
- establish foothold.

3) Expand network Access
- Expand access
- Escalate privileges
- Move laterally
- Conduct internal recon
- maintain persistence.

countermeasure : enforce strong user polices by enabling multi fa and restricting the ability to use same password across systems.

countermeasure: Analyze all traffic and endpoints, search for anomalous behaviour.

4) Attack gains strength - operational security
- Defense evasion and monitoring
- feedback pipeline.

5) Attack objective execution - Execute objective
- Establish your cyberattack strategy.

countermeasure: Thoroughly examine available forensics to understand attack details, establish mitigation priorities, provide data to law enforcement, and plan risk reduction strategies

⇒ Data Breach

involves data either belonging to the organization only but more often both inside and outside the organization.

↳ Key stats

→ 21% ransomware share of attacks
→ 17 months before ransonware gang rebrands or shuts down
→ 41% perant of attacks exploiting phishing for initial access
→ 33% increase in number of incidents caused by vulnerability exploitations from 2020 to 2021
→ 3 X click effectiveness for average targeted phishing campaigns that add phone calls.

→ 146% increase in linux ransomware with new code.
→ #1 manufacturing industry rank for attacks
→ 61% manufacturing share of compromises on OT-connected organizations. (36% of them were ransomware attacks)
→ 2204% increase in reconnaissance against OT

→ 74% share of IoT attacks originating from Mozi botnet
→ 26% share of global attacks that targeted Asia.

⇒ Anatomy of an attack - Lions at the watering hole

Step 1: stake out the watering hole
- insert iframe that redirects visitors to zero-day malware download

Step 2: Catch the visiting "gazelles"

Step 3: the prey returns to the herd.

⇒ Anatomy of an attack - Timeline

- July 13-15, 2012
  - Several regional consumer financial services websites are hacked
  - Hackers plant hidden iframe on consumer portal

- July 13-22, 2012
  - customers are redirected to malicious download site when they visit bank website.

- July 15-18, 2012
  - Infections detected at several companies

⇒ Anatomy of an attack - Vulnerable hosts were infected

- Attackers used different variants of Gh0st RAT remote access Trojan horse

⇒ Anatomy of an attack - Host response

- After being infected, compromised hosts made contact with remote command and control server in China.

⇒ Anatomy of an attack - risk of delaying a response to an attack

- If the attack isn't detected fast enough, infected machine becomes new launch point of deepening penetration

⇒ Prevention: Apply Big Data to Security intelligence and threat management

W2

⇒ Phishing scams

- phishing
- spear phishing
- whaling

↳ Common phishing tactics

- suspicious activity or log-in attempts noticed
- claim there's a problem with your account or payment info
- include a fake invoice
- want you to click on a link to make a payment
- offer coupon for free stuff.

↳ Impact

- financial cost of data breach is 3.86 million dollars
- phishing accounts for 90% data breaches
- 76% businesses reported being victim of phishing
- BEC scams accounted for over 12 billion dollars in losses.
  ↳ Business email compromise
- phishing attempts grew 65% between 2017 and 2018

→ Common type of identity theft : Credit card fraud.

M T W T F S S

Page No.: YOUVA

Date:

⇒ google and faubook phishing case study

- stole over 100 million dollars total from google and faubook
- set up fake business and send phishing email to employees.
- accused Rimasauskas posed as another company
  - served as sole number of board
  - [Taiwan based Quanta computer]
    - actually does business with faubook and google.

- Scam took 98 million dollars from faubook [2015]
- 23 million dollars from google [2015]
- Rimasauskas' work also involved "forged invoices, contracts and letters that falsely appeared to have been executed and signed by executives and agents" of the company he was impersonating

↳ Vulnerabilities

- Spear phishing : targets specific users or groups, in this case finance team.

- ~~Delayed Response : all the systems were bypassed~~
- Systems : all the systems were bypassed
- Delayed response: 100 mil taken due to lack of detection
- people: given the large usual transaction this team was.

used to facilitating, those requests were not unusual.

↳ Prevention

- Early detection
- reviews invoices
- implement 2fa
- email system automation
- employee education/training
- SPAM filter
- critical patches
- Antivirus
- Encryption

→ email system automation (from and reply addresses do not match then flag it)

⇒ Point of Sale Breaches

↳ The main point of POS is to steal your 16-digit credit card numbers.

POS: technology used to provide payment information in exchange for a good or service.

↳ Security control and processes for PCI DSS Requirements

1. Build and maintain secure network and systems
2. protect card holder data
3. Maintain vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test results
6. Maintain an Information Security policy.

↳ Being only PCI compliant is not enough...

→ Semi-Integrated approach (payment): sensitive card data is isolated, encrypted and sent directly from terminal to intended processing host or gateway. This way payment card data never touches POS.

→ Mobile device management: security software that allows businesses to remotely deploy and securely manage mobile POS solutions

→ point-to-point Encryption: Helps protect payment card data while in transit.

→ Tokenization: Replaces sensitive information with a secure encrypted token protecting it from cyber criminals when data is at rest.
Can only be decoded by payment processor.

→ Employee Education.

↳ POS Malware

- most POS softwares run on windows or linux, essentially making them a small computer.

- most POS malware comes equipped with backdoor and command and control features.

- Decryption of data occurs after transit on the sale device's RAM where its processed.
- POS malware specifically steals targets the RAM to steal unencrypted information, a process called RAM scraping

↳ Types of Malware

- Alina: scans system's memory to check if contents match regular expression, which indicate presence of card info.
- vSkimmer: If it doesn't find it server, it checks for presence of removable drive with label "KARTOXA007". If drive is found, it drops

a file that contains any stolen info into it, allowing offline data enfil.

- Dexter: not only steals card info, also steals various system info and installs keylogger onto affected systems.

- FYSNA: Using TOR Network to communicate with its C&C server makes its detection and investigation difficult by making all of the network traffic made by malware difficult to analyze.

- Decibel: checks if sandboxing or analysis tools are present on a machine before running.
This aims to make detection and analysis more difficult.

- BlackPOS: uses FTP to upload information to attacker's server. Allows consolidation of stolen data from multiple POS terminals on single server.

↳ POS Breaches prevention

- Actively monitor POS network
- limiting host that can communicate with POS systems
- adopting chip card enabled Pos terminals
- end-to-end encryption of cardholder data

↳ POS skimming

step 1: Criminal installs a hidden recording device that's able to read magnetic stripe on back of credit and debit card

step 2: The thief also installs a fake keypad overlay that looks and feels exactly like terminal keypad.

step 3: Customers swipe their cards and enter PIN

step 4: later uninstalls skimming gadgets and transfer all stolen data to his/her computer.

⇒ PoS Case study - Home Depot

↳ Pos Attack summary

- Attacker was using stolen credentials from one of the retailer's vendors
- Those creds were used to obtain acess to network, privilege elevated and acess to POS systems to record credit card details.
- The malware infection went unnoticed for 5 months between april and September 2014
- grabbed 56 million credit and debit card data
- grabbed 53 million email addresses
- Stolen card details were put up for sale, and bought by carders.
- Home depot began investigation on september 2nd.

↳ Vulnerabilities

- Attackers exploited a zero-day vulnerability in windows which allowed them to pivot from vendor specific environment to Home depot corporate environment.

(zero-day vulnerability: vulnerability unknown to party responsible in mitigating them)

↳ Countermeasures

- Vulnerability management program : no regularly scheduled scan
  : missing vulnerability

management system/program
: performing monthly vulnerability scans of POS environment

- Systems : configuration of hardware, software and network
: no proper segregation between home depot corporate and POS network
: POS environment should be in its own VLAN.
: network threat protection turned off.
: point-to-point encryption missing.
: POS running on windows XP → vulnerable to attacks

- Vendor credentials : credentials weren't properly managed.
: limit access rights for users to bare minimum permissions they need to perform their work.

- Delayed Response : lack of monitoring capabilities led to 5 months delay.
: capability of forwarding network or host activity in POS environment to a SIEM would have been benificial.

↳ Cost

- $19.5 million payout to customers.
- $134.5 million to credit card companies and banks
- $179 million for retail data breach
- $200 million → total cost

↳ Prevention

masks payment data uniquly for each transaction.

- chip-and-pin card is embedded with security chip in addition to traditional magstripe
- additional security provided by P2P encryption.
- alternative methods of payment → apple pay, google pay

never pass credit card info to margin.

W3

03/12/22

⇒ 3rd party Breach

↳ Supply Chain Attacks (aka- value- chain attacks or 3rd party attacks) are attacks originated from one of your third parties that has acess to your system. Which includes data management companies, law firms, email providers, web hosting companies, any external software or hardware used in your system.

↳ 41% of businesses encountered third party misuse of data

↳ 60% of all data breaches happen via 3rd party vendors.

Types of Breaches

- Cloud-Based (storage or hosting services)
- Payment (online payment or CC processing services)
- JavaScript library (web analytics collection)

NIST SCRM Guidance

- primary objective it to identify, access, and mitigate products and services that contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within cyber supply chain.

Best practices to avoid breach from 3rd party

- Evaluation of security and privacy practices of all third parties & conduct regular audit and assessments to evaluate security and privacy practices of 3rd parties.
- An Inventory of all 3rd parties with whom you share information - Track all 3rd parties that have access to sensitive data and how many parties are sharing data with others.
- Frequent review of 3rd party management policies and programs.
  regularly evaluate security and privacy practices of third party and nth parties.

- **Third party Notification** when data is shared with Nth parties - mandate that third parties provide information and transparency into their Nth party relationships prior to sensitive data.

- **Oversight** by the board of directors.

↳ 3rd party breaches - dominant security challenge - 63% of breaches linked to a third party.

- financial services → 2nd most 3rd party breaches
- Health and pharma → less likely
- Retails → most 3rd party breaches
- Technology and software → most likely

→ **Key findings**

- 3rd party breaches are expensive
- automated tools provide better results
- less proactive in mitigating 3rd party security gaps

→ **Vendor Issues**

- 1/3rd of respondents - mitigate or remediate security gap
- 28% would terminate relationship with vendor
- 1/3rd would work with 3rd party

→ Consumer impact

- loss of trust in business (65% lost trust; 80% defect)
- negative word of mouth (85% speak to others; 35.5% social media)
- lose out to competitors. (52% go for better companies)

⇒ Third party Breach Case study: Quest Diagnostics

↓

largest providers of clinical laboratory testing services in the US.

- Sensitive data of 11.9 million patients was accessed, ranging from credit card numbers to bank account information and even SSN.

↳ Timeline

- Unauthorized user gained access to Quest Diagnostic's sensitive data via billing collections vendor named American Medical Collection Agency.
- Hacker had access to information for 7 months from august 2018 to March 2019.
- AMCA discovered the breach on May 14 and reported it to Quest.

↳ Vulnerabilities

- Data protection of PII, medical and financial data.
- 3rd party auditing (lack of it)

  - unknown party gained elicit access to the AMCA website, and executed a MITM attack focused on payment page.
  - Attackers log payment and personal information entered by the visitors.

- Disclosure of Breach Data once discovered.

  - must provide notification of breaches to affected individuals, the secretary, and in certain circumstances to the media.

↳ Cost

- Several class action lawsuits against Quest Diagnostics at this time.
- exposed trifecta of data
  - PII,
  - medical conditions
  - financial account information.

↳ Prevention

- Evaluation of the security and privacy practices of all third parties
- inventory
- frequent reviews of 3rd party management policies and programs
- third party notification
- oversight by board of directors.

↳ Breach Plan

- https://securityintelligence.com/posts/latest-third-party-data-breach/

!! good and important reading.

- Indicators of compromise of 3rd party software
  - Outbound transmission of data going somewhere never gone before - red flag!
  - An application that changes or elevates privilege is another one.

⇒ Ransomware

- type of malware that infects computer systems, restricting users' access to the infected systems.
- Users files get encrypted and systems gets locked.

↳ Types of ransomware

- Crypto → encrypts all files
- locker → locks you out of your device
- leakware / Donware → blakmail to release footage or incriminating files

↳ Attack vectors

- phishing
- Remote Desktop protocol (RDP)
- Software vulnerabilities
- Malicious links

↳ Prevention

- Backup - Having a full backup of your files
- Update softwares and passwords
- Antivirus
- Beware of links

M T W T F S S
Page No.: YOUVA
Date:

Themes observed in ransomware incidents

- most common
  - RDP
  - Phishing
  - drive-by downloads
- Dwell time
  - 3 days passed between first evidence of malicious activity and deployment of ransomware
- After hours deployment.

Ransomware examples

- Locky
  - Encrypts over 160 file types
  - Uses phishing to target developer design file types.
- Troldesh
  - victim caught via spam email links and attached.
- WannaCry
  - Capitalizes on out of date software in healthcare industry
  - 4 billion in loses worldwide
- Bad Rabbit
  - Uses Adobe fake flash website to install ransomware
- Ryuk
  - disabled windows system restore button.
  - Encrypted network drivers as well.

M T W T F S S

Page No.: YOUVA

Date:

[cont.] ransomware examples

- Jigsaw
  - tormented victims by deleting files incrementally with each hour the ransom wasn't paid
- CryptoLocker
  - spread through email attachments
  - impacted half million computers
- Petya
  - Prewursor to Golden eye
  - encrypted entire hard drive
- Golden Eye
  - Targeted high profile users and locked them out completely.
- GrandCrab
  - claimed to have used the users webcam to record personal moments and threatened to release footage unless a ransom was paid.

↳ Jackware - goal of jackware is to lock up a car or another device until you pay up.

↳ part of Ransomware of Things

⇒ Ransomware Case study - City of Atlanta

- City of ransomware suffered a widespread ransomware attack in 2018
- breach shuttered many duvices in city hall for 5 days.
- virus used to attack the city was the SamSam ransomware
- To unlock city's systems and data, hackers demanded $51,000 in bitcoin.
- Denied ransom pay.

- Brute force ransomware
- Attacks weak infrastructure

↳ Timeline

- march 22, 2018
- Atlanta disabled wifi at airport until 2nd april
- City restored online water bill payment system in may
- court's online bill payment option and docket boards weren't returned until June.

↳ Vulnerabilities

- operations during an attack : no plan in plau if attack occured.
  - Business continuity and operational impact assessment was happening during attack.

- Readiness of systems

  - lack of spending upgrading infra
  - large number of vulnerabilities logged in a January 2018 audit

↳ Cost

- $17 million - cost taxpayers
- $6 million - security services and software upgrades
- $11 million - new resources like laptops, phones, etc

↳ prevention

- IT officials must know network architecture, invest in email infra, scrutinize email attachments and look for browser vulnerabilities
- multi-factor authentication and segmentation is crucial.
- Agencies should have backup plans and make it secure
- State and local governments should have security zones segmented well within own network so that they can't move laterally in their network even after brute forcing themselves through.

↳ Moving forward: City's approach to cybersecurity now rests on three pillars: 1) governance with compliance

M T W T F S S

Page No.: YOUVA

Date:

2) vulnurability management
3) overall threat management.