Security+ Notes 3

Social Engineering

- Manipulative strategy using psychology to gain access
- Manipulate to reveal confidential information
- Target human element
- Combat it with educating users of your company
- Motivational triggers
- Impersonation
- Pretexting
- Phishing attacks
- Frauds and scams
- Influence campaign
- Other Social Engineering Attacks

Motivational Triggers

- 6 types
    - Authority
        - The power or right to give orders, make decisions and enforce obedience
        - Most comply to whoever they believe has a position of authority to make requests
        - Someone convincing someone else they are important within a company or as a client
        - IRS scams call people scaring them to give them info so they dont come to their house
    - Urgency
        - Sense of time sensitivity that causes people to prioritize certain actions
        - Most people want to be helpful
            - Swipe your access badge to let someone with their hands full inside a sensitive area
        - People call the helpdesk claiming they are locked out of their account and need access to their computer right now
        - Urgency can cause a bypass of security procedures
    - Social Proof
        - People look to the behaviors of others to determine their own
        - Attackers use others online to spread the word about their scamming website
        - One friend can influence another
    - Scarcity
        - Pressure from feeling like something is in short supply, causing a quick reaction to something
        - “Sign up now, supplies are limited”

- Likability
    - People want to interact with people they like
    - Social engineers are typically likable and friendly to gain trust from others
    - Attractiveness can gain likability
    - Sexual Attraction
    - Pretending to be a friend
    - Common interests
- Fear
    - Feeling afraid of someone or something as likely to be threatening
    - " if you do not do this, something bad will happen to you"
    - Fear can be coupled with other motivational triggers
- Motivational triggers can be combined and used against individuals to gain information

Impersonation

- 4 main forms used by attackers
    - Impersonation
        - Adversary assumes the identity of another
        - Someone likable or with authority
        - First collect info on target org or users
        - Providing details helps make a lie more believable
        - Consequences
            - Unauthorized access
            - Disruption of services
            - Complete system takeover
        - Provide security awareness training
    - Brand impersonation
        - Attacker impersonates a company or brand
        - Emails
        - Uses logo, language, and identifiable info
        - To protect: educate on these threats, email gateways, monitor brands online presence
    - Typosquatting
        - Url hijacking
        - Cybersquatting
        - Taking a URL domain name that could be a typo of a popular website to create a scam against users who have misspelled the website URL
        - Combat it:
            - Orgs purchase and reserve common typo domains
            - Educate on this tactic
    - Watering Hole attacks
        - Compromise a specific site commonly used
        - Passive - does not attack target directly
        - To mitigate
            - Keep systems up to date

        - Educate
        - Advanced malware and detection tools

Pretexting

- You don't know anything about the org, but you give basic facts to trick someone to give you more information
- Common pretext calls
    - Your computer is infected with malware
    - Follow these steps
- Train employees to not fall for this
- Do not fill in gaps for people when they call

Phishing

- Different types
    - Phishing
        - Sending fraud emails seemingly from a reputable source aimed to get sensitive info from a user
        - Malicious links or attachments
        - Mass email campaigns in hope of someone trusting the link and email
    - Spear phishing
        - More targeted towards a indiv. Or organization
        - Higher level of customization
        - Like phishing but has a higher success rate
        - Attacker can pick contact info from a targeted data leak to narrow and specify the information in the scam to make it more believable
        - Tailored to recipients
    - Whaling
        - Targets high profile individuals
        - Executives or board members within a company
        - Lots of prep and precision
        - Massive financial gains
            - Targets have the ability for large transfers of money
    - Business Email Compromise
        - Using an internal email account to gain information from the other employees within a company
        - Impersonate a senior exec or trusted partner
            - Seemingly convincing requests for wire transfers or confidential data
            - Relies on trust
            - Often leads to financial losses
    - Vishing
        - Sharing personal info over the phone
        - Typically impersonates bank or gov agency
        - Most people are friendly
            - Gaining trust
    - Smishing

        - SMS phishing
        - Links to fraudulent website
        - phone numbers to call to create a sense of urgency

Preventing Phishing Attacks\

- Phishing is one of the most persuasive attacks
- User security awareness training
- Anti-phishing campaign
    - Educates about risk from phishing and how to identify it
- Organizations should conduct regular training on the different phishing techniques
- Common characteristics of emails
    - Generic greeting
    - Grammar and spelling
    - Spoofed addresses
- In depth remedial training for those who fall victim to a phishing attack
- Common indicators
    - Urgency
        - Prompt recipient ro react quickly
        - “Click now to claim your prize before expire”
    - Unusual Request
        - Passwords
        - Credit card numbers
        - Your bank would never ask for sensitive info over an email or phone call
        - Your IT would never contact you asking for your login info
    - Mismatched URL
        - Display text can mask where the link will actually take you
        - Check the link by hovering mouse over the url and see if the link matches the url
    - Strange Email Addresses
        - Always verify the sender's email
        - Hover over the display or double click
        - Make sure the email matches the display name
        - Red flags: does not match or address is unusually long
    - Poor Grammar and Spelling
        - Poor english, grammar and spelling errors are common in phishing campaigns
        - People can get through this by using AI to proof read to hide their tracks
        - Some attackers include errors to not overwhelm themselves with too many users using their links all at the same time
- Promptly report suspicious messages to protect against potential attacks
- If you're analyzing attacks, first start with the messages and try to identify common indicators
- Inform all users about the threat
- If the campaign was successful, still use the incident to review and update countermeasures and awareness training

Conducting Anti-Phishing Campaign

- Create your own email
- phishinsight.trendmicro.com
    - Free tool for creating a campaign
- Recipient list (name, email, title/department)
- Decide on a template
    - Ex. linkedin request
- Specify the sender
- Set up schedule for how long or extensive you want your campaign to be
    - See if your company learns over time
- Decide on consequence from clicking on a link
    - Link remedial training

Frauds and Scams

- Fraud
    - Wrongful deception intended for financial or personal gain
    - Tricked to handing over valuables rather than them being taken away from you (theft)
    - Identity Fraud
        - Use of another's information to commit a crime or deceive or defraud that person or another
        - Attacker charges someone else's card number
    - Identity Theft
        - Stealing another identity and using as their own
        - Impersonate the victim and apply for a new card or account
        - Attacker fully assumes the victim identity
- Scam
    - Someone tries to deceive a victim to do something
    - Invoice scam
        - Someone tricked to pay an invoice for something they did not order
        - The invoice becomes legitimate once the victim confirms the order ovber the phone so they become trapped in an overpriced payment for something they did not order
    - Analyze pdf invoices by scanning them

Influence Campaigns

- Powerful tool for shaping public behavior
- Breeding ground for disinformation
- Coordinated to affect public perception
- Public health campaigns (benign)
- Spread of false information for public opinion (malicious)
- Typically high level adversaries
    - Nation state actors
    - Hacktivist groups
- Misinformation
    - Unintentional spread

        - Ex. people hearing that gargling salt water can kill COVID -19
    - Disinformation
        - Intentional spread with intent to deceive
        - Example: other countries spreads disinformation to influence elections
        - Russian creating fake accounts on twitter to influence the electoral process
        - Bitcoin scan 2020
            - Twitter breach (high -profile accounts were taken over)
            - Accounts posted a bitcoin scam
            - Reliance on the legitimacy of the account lead to loss of money to victims
            - Motivations do not always have to be political
    - How to combat campaigns
        - Media literacy
        - Transparency
        - Regulation

Other Social Engineering Attacks

- Diversion Theft
    - Manipulating a situation to steal valuable items or info
        - Diverting traffic to steal a victims data
        - DNS spoofing
            - DNS settings is manipulated to direct to a fake website
            - User prompted to enter sensitive info
- Hoax
    - Malicious deception spread to social, email, or other com channels
    - Often paired with phishing/impersonation attacks
    - Use good critical thinking a fact checking of websites and sources of communication
- Shoulder Surfing
    - Looking over another's shoulder for information
    - Targets do not need to be close
        - Cameras
    - Be aware of surroundings before accessing sensitive info
        - Privacy screens
- Dumpster Diving
    - Searching through trash for valuable info
    - Shred sensitive docs
    - Virtual DD
        - Attacker looks in deleted or recycling files and rewrites them
- EavesDropping
    - Secretly listening to private convos
    - Wiretapping
    - Adversary in the middle
        - Perp intercepts communication between two unaware parties
    - Secure communication channels
    - Encryption

        - Patch systems
- Baiting
    - Leaving a malware infected device in hope someone plugs in the device to their computer and install the software
    - Train to never use a device if you do not know where it came from
- Piggy backing or tailgating
    - Following another in a secure environment
    - Tailgating
        - Following another without their knowledge
    - Piggy Backing
        - Convincing someone authorized to let them in using their credentials to be helpful