Overview of Attacks

geotagging

A business design choice of enabling geographic information to be saved
Could include employee actions and whereabouts
Location of stock
Warehouse to door tracking information

Threat Hunters Handbook

BOARD GAME

https://github.com/asos-hs
https://medium.com/@harjitsandhu

Overview of Attacks

phishing

A social engineering mechanism of stealing data from an unsuspecting person
Could be a fake log in page to harvest credentials
Could be a fake purchase page to steal credit card information

Demo USBs

A social engineering mechanism of allowing an attacker access to an employees machine

The free USB may have a trojan/virus/ransomware

help desk spoofing

A social engineering mechanism where an attacker would contact an employee and act as help desk

Could be leveraged as a way in if the employee carried out actions on behalf of the attacker

Overview of Attacks

vulnerability checks

A reconnaissance mission
can show weaknesses to the systems
can highlight ways people have attacked an won

zero day

A mechanism that allows an attacker (via some trusted library) the ability to add malicious code

Could be maliciously added by a dev

Query string hacking

a mechanism that the attacker can abuse, which allows him to manipulate the serer by manipulating the query string

Overview of Attacks

privilege escalation

A mechanism whereby you gain more access than you are allowed
A Dev getting admin access, or network access
A network admin getting repository access
They May be able to change things in areas that aren't theirs

cross site scripting

A mechanism that allows an attacker the ability to insert scripts

May be able to add scripts to the customer facing site

Maybe able to add scripts to bac end systems

session hijacking

A mechanism that allows an attacker to steal a user session from a user in real time

May be able to act on behalf of the user

Overview of Attacks

Disgruntled employee

This person is upset at the business
May want to steal data
May want to steal stock
May want to steal money
Has access to internal systems
May be coordinating with collages

careless employee

This person just made a mistake

May inadvertently deleted/shared/approved something

lost mobile phone

This person simply lost their phone

May have had emails or text messages on there

May have sensitive phone numbers on there

Overview of Attacks

physical access

Can people just walk in and plug in a computer
Are they able to access the wifi from outside the building

web browsing

Employees browsing the web, could land on a malicious site, and download a malicious package

weak infrastructure

A Poor security policy that allows for poor infrastructure

This could be weak firewall configuration

Old vulnerable operating systems

Open wifi

Overview of Attacks

patching

A Poor security policy that allows for updates not being run
can result in well known exploits and vulnerabilities being known

weak passwords

Maybe the password policy for staff or customers is weak

Maybe there are no back off periods after incorrect tries.

denial of service

A mechanism that could disrupt business

May be able to cause financial impact

Maybe trying to damage reputation during large sales