4 KWETSBAARHEDEN & MAATREGELEN

- **Kwetsbaarheid:**

  -> is een eigenschap van ICT, een organisatie of gebriuker die actoren kunnen misbruiken om hun doelen te bereiken of die door een natuurlijke of technische gebeurtenis kan leiden tot verstoring.

- **Actoren:**

  -> zijn individuen, instellingen of organisaties die van doorslaggevende invloed kunnen zijn in een bepaald proces. Hierbij gaat het om het proces van cybercrime.

4.1 ORGANISATORISCHE ONTWIKKELINGEN

Er is steeds meer publiciteit rondom technische kwetsbaarheden.

- **Heartbleed:**

  -> door kwetsbaarheid in OpenSSL konden aanvallers op afstand het interne geheuigen van systemen uitlezen

  -> speciaal geconstrueerd verzoek naar een 'beveiligde' server sturen, zodat server min of meer een willekeurig deel van zijn geheugen terugstuurt.

  -> dit geheugen kan gebruikersnamen, wachtwoorden en private keys van beveiligingscertificaten teruggeven

  ANDERE KWETSBAARHEDEN DIE BEKEND GEMAAKT ZIJN

  - **Shellshock:**

    -> op afstand commando's uitvoeren op geïnfecteerde systemen.

  - **POODLE:**

    -> om in te breken in beveiligde verbindingen die gebruik maakten van SSL_{v3}

  - **FREAK:**

    -> door deze kwetsbaarheid konden aanvallers het beveiligingsniveau van beveiligde verbindingen verlagen

4.1.1 cloudinfrastructuur als extensie van het bedrijfsnetwerk

-> individuele gebruiker moet zelf beveiligingsmaatregelen nemen

-> beveiliging van de cloudservice zelf kan ook kwetsbaar zijn

-> toegang tot clouddiensten en de opslag van data moeten goed beveiligd worden

-> vergroot kans op spionage of overtreding van de privacywetgeving door internationale karakter

4.1.2 up-to-date blijven

-> kwetsbaarheden in software worden door leveranciers opgelost door het uitbrengen van updates. Als software niet up-to-date is, blijven kwetsbaarheden aanwezig

4.1.3 gebruiker als kwetsbaarheid

-> technische ontwikkelingen hebben laten zien dat het riskant is te vertrouwen op gebruikersbewuustzijn als basis voor het oplossen van kwetsbaarheden

4.1.4 phishing

-> kwaliteit van phishingteksten is teeds beter geworden

-> moeilijk om phishing met e-mail filtering tegen te houden, het komt ook immers binnen op privé-accouunts

4.1.5 inloggegevens voor de cloud vormen een zwakke schakel

- **Fappening-incident (combo van 'fap' = masturbatie en 'happening'):**

-> aanvallers hadden gebruik gemaakt van zwakke wachtwoordversleutelmechanismes om toegang te krijgen tot foto's

-> dmv tweestapsverificatie werden deze mechanismes nadien beter beveiligd

-> er werden 500 privéfoto's van beroemdheden op het 4-chan platform gegooid

-> door fout in API van de iCloud kon er onbeperkt geraden worden naar de wachtwoorden

4.2 TECHNISCHE ONTWIKKELINGEN

4.2.1 kwetsbaarheden in firmware

-> steeds moeilijker te detecteren

-> bij insteken van een USB-stick kan een pc al geïnfecteerd worden

-> firmware op harde schijf kan worden misbruikt

-> daarnaast bevat de pc zelf ook firmware om op te starten waar kwetsbaarheden inzitten

4.2.2 mobiele telefonienetwerk

-> kwetsbaarheid hierin heeft te maken met het SS7-protocol dat providers gebruiken om gesprekken aan elkaar door te geven.

->het was voor de aanvaller mogelijk om gesprekken en SMS te onderscheppen

4.2.3 toegang tot en opslag bij clouddiensten

-> het beveiligen de toegang tot en de opslag van data bij clouddiensten

-> slecht beveiligde cloud verhoogt het risico op spionage of overtreding van de privacywetgeving, misbruik wordt steeds geavanceerder en moeilijk te herkennen

4.3 MAATREGELEN

Maatregelen kunnen genomen worden om technische kwetsbaarheden te beperken. Maatregelen kunnen preventief of reactief van aard zijn en zijn gericht op de mens of de techniek

4.3.1 de mens

-> de mate waarin men zich bewust is van de aanwezige belangen, kwetsbaarheden en dreigingen en de manier waarop men omgaat met risico's die hiermee samenhangen, spelen een cruciale rol in de weerbaarheid van de mens tegen aanvallen

4.3.2 bewuste en bekwame gebruuikers gedragen zich veiliger

-> meer antivirus-systemen installeren

-> minder geneigd zijn om persoonlijke informatie in te voeren

-> gebruik verschillende wachtwoorden en open geen emails van onbekende mensen

4.3.3 organisaties hebben moeite voldoende cyberprofessionals aan te trekken

-> cybersecurity moet vanuit verschillende disciplines worden benaderd

-> oriëntatieniveau van de functies variëren: strategisch, tactisch en operationeel

-> aansluiting van het onderwijs op de arbeidsmarkt is onvoldoende

4.4 TECHNISCHE OPLOSSINGEN

- **Tweefactorauthenticatie wordt populair:**

  -> door makkelijke paswoorden kunnen kwaadwillende gemakkelijk toegang krijgen

  -> 2FA voorkomt dat de aanvaller door phishing of het raden van je wachtwoord toegang krijgt tot je account

  -> je krijgt een speciaal gegenereerde code via sms toegestuurd dus aanvaller heeft je gsm nodig om in te loggen

- **De sleutelrol van cryptografie:**

  -> speelt een sleutelrol in technische beveiliging

  -> met cryptografische protocollen kan informatie versleuteld worden, doorgaans gebeurt dit wanneer de informatie over wordt verzonden of opgeslagen.

  -> Hier zitten kwetsbaarheden in

  - **Transport Layer Security (TSL):**

    -> is een protocol voor opzetten en gebruiken van een cryptografische beveiligde verbinding tussen 2 computersystemen

    -> dit wordt gebruikt in oa webverkeer, e-mailverkeer en bepaalde VPN-netwerken

  - **DNS Security Extensions (DNSSEC):**

    -> er wordt bij gebruiuk van deze cryptografische beveiliging gecontroleerd of het gegeven antwoord authentiek is van de juiste bron

    -> BV op ingetikte domeinnaam, zo kunnen gebruikers veridiëren of ze op de juiste website zitten

  Detectiecapaciteit is essentieel om geavanceerde aanvallen te ontdekken

  - **Advanced Persitent Threats (ATP's):**

    -> richten zich op organisaties en omzeilen structureel bestaande beveiligingsmaatregelen

    -> zeer moeilijk te detecteren en bij detectie en verwijdering van de initiële malware wordt op een andere wijze hetzelfde doelnetwerk binnengedrongen

    -> ook beveiliging van open source software kost veel geld

    -> het core infrastructure initiative stelt geld ter beschikking om projecten te ondersteunen die de basisbeveiliging van het internet ondersteunen.

  - **Responsible disclosure:**

    -> op verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie, openbaar maken van ICT-kwetsbaarheden op basis van een vast beleid

Er zijn websites gelanceerd en discussiesessies georganiseerd om dit beleid te bevorderen

PREVENTIEF

-> bewustwording

-> vaststellen van kwetsbaarheden

-> opstellen van protocollen

- ICT-protocol (email en internetprotocol werknemers)
- Cybercrime-protocol
- Datalek-protocol
- Inval(bezoek) opsporingsinstanties protocol
- Meewerken aan inlichtingenverzoeken protocol

-> tijdelige herkenning

-> goede beveiliging van hardware en software: cybersecuritybeleid

4.5 DE MEEST VOORKOMENDE VORMEN VAN ONLINE CRIMINALITEIT

4.5.1 virussen / malware

-> meest voorkomende vorm van cybercrime door installeren kwaadwillige software

-> malware is verzamelnaam voor kwaadaardige software

-> woord is samenvoeging van het engelse 'malicious software'

- **Wat te doen?**

-> Installeer nooit software van onbekende partijen

-> installeer een antivirussoftware

4.5.2 ransomware

-> vorm van malware die je computer blokkeert

-> gebruikt als chantagemethode

-> openbaar maken van pornowebsites die mensen hebben bezocht

-> versleutelen van persoonlijke bestanden

- **Wat te doen?**

-> geen speciale trucjes om je te beschermen tegen ransomware

-> behalve updaten van je systeem

4.5.3 cryptoware

-> vorm van malware die je bestanden onherstelbaar vernietigd:

-> financiën, klantenbestanden en foto's zijn de eerste doelwitten

-> criminelen vragen losgeld om in ruil daarvoor de bestanden weer beschikbaar te maken

- **Wat te doen?**

  -> regelmatig back-ups maken en deze op een aparte schijf bewaren

  -> een remedie achteraf is er niet

4.5.4 hacken

-> beveiliging van je software wordt omzeild

-> twitter-accounts die worden gehackt, hacken van DigiD en DDoS-aanvallen op banken

- **Wat te doen?**

  -> beveilig je foto's in de cloud

  -> gebruik sterke wachtwoorden

  -> stel tweestapsverificatie in

4.5.5 visueel hacken

-> criminelen verzamelen informatie door naar scherm slachtoffer te kijken (schoudersurfen)

-> groeiend probleem omdat pc's en laptops vaker in openbare ruimtes gebruikt worden

- **Wat te doen?**

  -> schermfilter van 3M verkleint de hoek van de computer, meekijken wordt vermoeilijkt

4.5.6 identiteitsfraude & phishing

-> aanvallers misbriuken gegevens om zich voor te doen als iemand anders

-> vaak worden abonnementen afgesloten of rekeningen op iemand anders naam afgesloten

-> voorkom dit door sterke wachtwoorden te gebruiken en erop te laten welke info je online deelt

-> veel gebriukte manier om aan je info te komen is phishing, hierbij wordt via vervalste websites of e-mails gevraagd om je gegevens

- **Wat te doen?**

-> dubbele beveiliging op je accounts, extra controlecode per sms of via app

-> online kopen/verkopen, stuur geen kopieën van je ID

-> wees voorzichtig op social media, zo brengen ze je profiel in kaart

-> indien toch gehackt, doe aangifte bij het meldpunt identiteitsfraude

4.5.7 identiteitshack

-> hierbij wordt iemands naam, profielfoto en andere persoonlijke informatie gekopieerd en misbruikt op het internet

-> iemands privacy wordt hierbij ernstig geschaad, bovendien grenst deze laster aan cyberpesten

- **Wat te doen?**

Zie hierboven bij identiteitsfraude

4.5.8 klikfraude

-> onlineoplichting waarbij nepadvertenties worden getoond, hoe vaker op zo'n advertentie wordt geklikt, hoe meer adverteerders betalen

-> via geïnfecteerde netwerken worden de verdiensten doorgesluisd naar criminelen

-> oprichten van neppagina's en –berichten

- **Wat te doen?**

-> melding maken bij desbetreffende advertentieprovidor, zoals adsense van google

4.5.9 grooming

-> digitaal kinderlokken

-> het doel is contact leggen met kinderen door volwassene. Doel is seksueel contact

4.5.10 koop- en verkoopfraude

-> kopen en verkopen via internet wordt gefraudeerd

-> betaalde spullen die niet geleverd worden

- **Wat te doen?**

-> als koper voorstellen dat je het geld cash wilt komen afgeven, aan de hand van zijn antwoord kan je al snel afleiden of hij hiermee wilt instemmen

Hieronder volgen enkele tips om je online veiligheid te vergroten:

-> gebruik sterke wachtwoorden

-> zet zo weinig mogelijk persoonlijke informatie online

-> maak zo weinig mogelijk gebruik van openbare wifi

-> koppel accounts niet aan elkaar

-> maak regelmatig back-ups

-> versleutel de data op je apparaten

-> gebruik, zeker bij internetbankieren een beveiligde website (https)

-> geef nooit informatie over je bankrekeningnummer, pincode of pasnummer via telefoon, email of aan iemand die zegt dat hij bij de bank werkt

-> heb je een email ontvangen van een onbekende afzender? Klik niet op de links

-> google anoniem

-> zorg voor een goede up-to-date virusscanner

-> gebruik geen internet explorer, gebruik chrome of brave

-> gebruik geen windows xp, deze is niet meer veilig

-> beveilig je smartphone

-> controleer regelmatig je accountgegevens en update indien nodig

- **Anoniem googelen:**

  -> als je incognito surft worden je zoekgeschiedenis niet opgeslagen net als de zoekopdrachten

  -> coockies en andere trackingsinformatie worden ook niet opgeslagen

  -> vereiste is wel dat je niet bij google moet zijn ingelogd, de cloud kan dan alsnog informatie over je browsegedrag opslaan

  -> werk met een Virtual Private Network

- **Beveiliging van je website:**

  -> **gebruik paswoord manager:**

  - Laat een password manager complexe wachtwoorden bedenken en opslaan in zijn kluis
  - Wachtwoorden worden opgediept wanneer je ze nodig hebt

  -> **update CMS en software:**

  - Gebruik je wordpress of drupal? Is het zinvol om deze voortdurend up te daten
  - Zo worden de lekken die hackers misbruiken gedicht
  - Verouderde software bevatten ook lekken, check regelmatig op updates bv met Ucheck

  -> **installeer security plug-ins:**

  - Voor bijna elke CMS zijn er plug-ins die je site veiliger maken
  - Ze blokkeren hackers na een paar inlogpogingen en rapporteren mogelijke aanvallen

  -> **activeer antivirus:**

  - Laat op achtergrond steeds antivirus draaien
  - Basisversie van AVG antivirus is gratis en eenvoudig
  -

4.6 VORMEN VAN HACKING

- **Classificaties:**

  -> verschillende subgroepen van de computer underground met verschillende motieven gebruiken verschillende termen om zich van elkaar te onderscheiden, of proberen een specifieke groep uit te sluiten waarmee ze het niet eens zijn.

  -> hackers zelf leggen meer nadruk op een spectrum van verschillende categorieën, zoals **White Hat**, **Grey Hat** & **Black Hat**

- **Aanval:**

  -> een typische aanpak in een aanval op het met het internet verbonden systeem is:

  a. **Netwerkregistratie**: informatie ontdekken over het beoogde doel
  b. **Kwetsbaarheidanalyse**: identificatie van mogelijke manieren van aanvallen
  c. **Exploitatie**: poging om het systeem in gevaar te brengen door gebruik te maken van de kwetsbaarheden die zijn gevonden via de kwetsbaarheidsanalyse.

- **Deel 1 targeting:**

  -> bepaalt op welk netwerk hij/zij in deze fase moet inbreken

  -> doel kan politiek of persoonlijk belang zijn of willekeurig worden gekozen

  -> vervolgens netwerk scannen om te bepalen of het kwetsbaar is

  -> alle poorten op een hostmachine testen om een reactie te krijgen

  -> open poorten, dit zijn degene die reageren, geven een hacker toegang tot systeem

- **Deel 2 Onderzoek en informatie verzamelen:**

  -> het doel op één of andere manier bezoeken of daarmee in contact treden in de hoop essentiële informatie die hem helpt toegang te krijgen tot systeem

  -> eventueel 'dumpster diving': hierbij gaat een hacker letterlijk door het afval van het bedrijf in de hoop documenten te vinden die belangrijke informatie bevatten.

  -> door middel van 'social engineering' bv zich voor te doen als iemand van de ICT-dienst en te vragen achter inloggegevens

- **Deel 3 Afronding van de aanval:**

  -> stadium waar het voorlopige doelwit zal binnengaan

  -> vele hackers zullen na dit punt worden gelokt in of gegrepen worden door gegevens die ook wel een honeypot genoemd wordt (een val die wordt opgesteld door computerbeveiligingspersoneel)

- **Voor de verschillende vormen van hacking kijk je op pagina 79 – 88**

4.7 SAMENWERKING

Fraude met behulp van malware wordt met succes teruggedrongen. Interbancaire detectiesystemen kunnen malware steeds beter automatisch detecteren en voorkomen.

- **Strijden tegen botnets (neerhalen en data delen):**

  -> GameOver Zeus-botnet is een vb van een botnet dat door samenwerking werd neergehaald

  -> echter wordt er wel getwijfeld of het wel succesvol is om botnets als GameOverZeus uit te schakelen omdat andere botnets de gaten die het neergehaalde botnet achterlaat terug opvult.

  -> Abuse Information Exchange heeft als doel informatievoorziening over botnets te verbeteren. Ze verzamelen data op een centraal punt, zo kunnen botnetbesmettingen beter en sneller worden bestreden.

- **Delen van dreigingsinformatie helpt om capaciteit efficiënt in te zetten:**

  -> door continu de systemen en applicaties in een netwerk te monitoren kunnen dreigingen vroegtijdig gedetecteerd worden en kan er snel ingegrepen worden

  -> dit is arbeids- en kostenintensief.

  -> door dreigingsinformatie te delen kunnen organisaties met minder inspanning een completer beeld krijgen van de dreigingen en hierop reageren

- **Regulering:**

  -> in 2015 is het wetsvoorstel meldplicht voor datalekken aangenomen, deze meldplicht wil datalekken door inbreuken op de beveiliging voorkomen.

  -> als deze zich toch voordoen is het de bedoeling om de gevolgen voor betrokkenen te beperken, het niet melden wordt bestraft met een bestuurlijke boete

  -> er wordt ook aandacht besteed aan de manier waarop organisaties hun weerbaarheid verhogen. Ondanks uitgebreid cybersecuritybeleid, maar door snel veranderende dreigingslandschap is de dekking hiervan niet altijd volledig.

  -> het platform internetstandaarden heeft als doel gebruik van moderne internetstandaarden te stimuleren en daarmee het internet voor iedereen betrouwbaarder te maken.

De overheid en het bedrijfsleven investeren in de versterking van de digitale weerbaarheid en de bescherming van belangen. Er is hierbij aandacht voor de menselijke factor, voor de technologische middelen en voor de samenwerking met anderen. Doordat het dreigingslandschap steeds meer verandert is het van belang dat organisaties hun beleid en maatregelen regelmatig herzien. Monitoring, detectie en respons zijn ook essentieel.

- Een **cybercriminoloog** die door een bedrijf **wordt ingeschakeld om advies te geven** over cybercrime en beveiliging, kan het bedrijf de **volgende belangrijke vragen voorleggen:**

  -> Worden er backups gemaakt en zijn deze al wel eens getest?

  -> Welke logbestanden zijn beschikbaar en wanneer roteren deze?

  -> Wordt de e-mail gearchiveerd, of alleen lokaal opgeslagen op computers?

  -> Worden telefoongesprek gegevens gelogd / eventuele SMS'jes

  -> zijn er proxyservers en welke informatie slagen deze op?

  -> BYOD

  -> Werkstations / thin clients

Hieronder volgt een casussituatie:

- Een **cybercriminoloog** wordt door dit bedrijf **ingeschakeld om uit te zoeken wat er gebeurd is**. Daarbij dient hij/zij de **volgende vragen te stellen en beantwoord te zien krijgen**:

  -> Wie host de website?

  -> Is de website in eigen beheer, of wordt deze onderhouden door een andere partij?

  -> Welke loggegevens zijn voorhanden?

  -> Hoe lang gaan de loggegevens terug?

  -> Worden er back-ups gemaakt van de server?

  -> Wie had er allemaal toegang?

  -> Hoe complex zijn de wachtwoorden?

Ook dient het bedrijf zich ervan bewust te zijn welke data naar buiten gaan en waar en naar wie het precies terecht komt:

-> OUTSOURCING / CLOUD -> INTERNET -> GMAIL / OFFICE 365 / TWINFIELD