3 DREIGINGEN

3.1 ONTWIKKELING, BELANGEN, DREIGINGEN & WEERBAARHEID IN CYBERCRIME

3.1.1 kernbevindingen

- **Cryptoware en andere ransomware is het cybercriminele bsinessmodel bij uitstek**

  -> criminelen blokkeren met cryptoware (gijzelvirussen) de toegang tot gegevens met behulp van encryptie

  -> geopolitieke spanningen manifesteren zich steeds vaker in inbreuken op digitale veiligheid.

  -> staten en andere actoren maken steeds vaker gebruik van digitale aanvallen en cyberoperaties

  -> digitale aanvallen hebben een grote omvang, daders zijn moeilijk te achterhalen en het gaat om lage kosten.

- **Phishing:**

  -> veel gebruikt in gerichte aanvallen

  -> phishingmails zijn voor gebruikers in gerichte aanvallen nauwelijks te herkennen

  -> met geslaagde campagne krijgen hackers toegang tot interne netwerken van organistaties en de daarop opgeslagen informatie.

  -> belangrijke maatschappelijke processen vallen stil als de bijhorende ICT-systemen en analoge alternatieven niet beschikbaar zijn.

Ransomware en cryptoware zijn malware die de ICT-systemen ‘gijzelen’ door ze niet beschikbaar te maken en waarbij om losgeld gevraagd wordt.

- **DDoS-aanvallen:**

  -> blijven plaatsvinden, maatregelen voorkomen vaak echter verstoringen.

- **Spearphishing:**

  -> hierbij gaat het om onbevoegde toegang tot gevoelige info van een organisatie of een privepersoon

3.1.2 dreigingen & maatregelen

-> grootste dreiging blijft uitgaan van beroepscriminelen en statelijke actoren.

-> criminelen die opvallen door goede organisatie, nauwkeurige uitvoering en technische geavanceerdheid.

-> terroristen vormen voorlopig nog geen grote dreiging.

-> conflicten, aanslagen en incidenten vormen context voor digitale aanvallen.

-> phishing en in het bijzonder spearphishing is hét middel voor gerichte aanvallen.

-> malafide advertenties blijven een gevaar voor internetgebriukers.

-> phishing kan niet alleen met bewustwording bestreden worden. De kwaliteit van de phishingteksten is steeds beter geworden.

-> beveiliging van open source software kost geld.

- **Heartbleed:**

  -> ernstige kwetsbaarheid in programmeerbib OpenSSL die in veel webservers wordt gebruikt.

  -> via internet het geheugen van systemen uitlezen die de kwetsbare openSSL detecteren.

  -> hierdoor kunnen sleutels gelezen worden

  -> webservers identificeren

  -> zorgen voor versleuteling van wachtwoorden, gebruikersgegevens en de inhoud van de webserver zelf.

  -> aanvaller kan data stelen zonder dat deze ontdekt wordt.

  -> detectieapparaat is essentieel om geavanceerde aanvallen te ontdekken.

- **Advanced Persistent Threats (APT's):**

  -> lastig te detecteren

  -> aanvallen zijn gericht op organisaties in verschillende sectoren, omzeilen structureel bestaande beveiligingsmaatregelen.

  -> nieuwe toepassingsgebieden leveren kwetsbaarheden en debat op. Bv besturing van vliegtuigen via cybersystemen etc.

- **De hoofdvragen in het CSBN (cybersecuritybeeld Nederland) zijn:**

  -> welke gebeurtenissen of welke activiteiten van welke actoren kunnen ICT-belangen aantasten?

  -> welke hulpmiddelen gebruiken zij en welke ontwikkelingen doen zich daarbij voor?

  -> in hoeverre weerbaar tegen kwetsbaarheden in ICT, kunnen die leiden tot aantasting van ICT-belangen?

  -> welke belangen worden in welke mate geschaad door beperkingen van de beschikbaarheid en betrouuwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die info en welke ontwikkelingen doen zich daarbij voor?

- **Manifestatie:**

  -> wanneer belangen worden geschaad, omdat een dreiging manifest wordt.

  -> weerbaarheid is dan onvoldoende

  -> kwaadwillende actor kan zo actief gebruik maken van een kwetsbaarheid in een systeem.

  -> manifestaties kunnen ook plaatsvinden door fouten van gebriukers en beheerders of door technische storingen

3.1.3 verstoring van ICT

- **Ransom- & Cryptoware:**

  -> gijzelt systemen door ze niet beschikbaar te maken

  -> hier wordt om losgeld gevraagd

  -> cryptoware versleutelt daarnaast de opgeslagen gegevens

- **Sabotage:**

  -> hoogst uitzonderlijk

  -> websites zijn enige tijd onbruikbaar of onbereikbaar

  -> meest voorkomende aanvallen = DDoS en defacements, of gegevens worden gewist

- **DDoS (Distrubuted Denial of Service):**

  -> motief blijft meestal onbekend

  -> zijn een gemakkelijk in te zetten middel

- **Defacement:**

  -> bij ontdekte kwetsbaarheid plaats aanvaller boodschap op de website met de melding dat hij gehackt is

  -> ideologische boodschap meestal

  -> ook wel benoemd bij het kapen van iemand zijn facebook pagina

3.1.4 malwarebesmettingen

- **Besmetting door advertentiesite:**

  -> uitval ICT, storingen zonder dader kunnen zorgen voor een verlaging van de beschikbaarheid van diensten.

  -> storingen van deze aard kuunnen minstens even grote gevolgen hebben dan moedwillige.

- **Digitale spionage:**

  -> voorgaande manifestaties vooral gericht op ICT

  -> bij spionage vooral gericht op het verkrijgen van informatie over slachtoffer.

- **Digitale oorlogsvoering:**

  -> opbouw van dergelijke kennis en infrastructuur kost veel tijd.

  -> daadwerkelijke inzet brengt significante juridische, politieke en morele implicaties met zich mee

  -> desondanks wel groeiend aantal cyberoperaties en digitale aanvallen met een politiek-militair doel waargenomen

- **Hybride oorlogvoering:**

  -> gebruik gemaakt van combinaties van alle mogelijke middelen die op de situatie worden toegespitst om maximaal rendement te behalen tegen minimale kosten.

  -> waaronder politieke, economische en/of militaire middelen inclusief cyber capaciteit

3.1.5 economische spionage bij bedrijven

- **Diefstal van informatie:**

  -> wanneer aanvallers data stelen met als doel deze met winst te verkopen, te publiceren of voor activistische doeleinden te misbruiken.

- **Diefstal van financiële middelen:**

  -> datasets bemachtigen en vervolgens voor veel geld te verkopen.

  -> stelen van geld door het inzetten van malware

3.2 ACTOREN: PERSONEN DIE DE SYSTEMEN AANTASTEN

- **Beroepscriminelen:**

  -> intentie is verdienen van geld en werkwijze van criminelen verandert voortdurend en is innovatief.

  -> hoge mate van geografische spreiding.

  -> dit maakt internationale samenwerking noodzakelijk

  -> zijn bereid om veel tijd te investeren in voorbereiding van digitale aanvallen.

  -> meer geduld in de uitvoering

  -> creatiever met het verzilveren van gestolen gegevens

  -> point-of-sale-malware richt zich op verkooppunten met pinpassen

  -> in de VS richtten criminelen zich op datadiefstallen in medische sector

  -> leveren diensten: cybercrime as a service

- **Statelijke actoren:**

  -> minder bekend

  -> dit zijn andere landen bv inlichtingendienst van de overheid

  -> vormen een probleem voor de nationale veiligheid en economie wordt bedreigd

  -> vormen aantrekkelijk alternatief voor spionagemiddelen

  -> dit soort aanvallen hebben een grote inpak

  -> niet statelijke actoren: civiele maatschappei, multinationale organisaties, bedrijven en religieuze groeperengen

- **Terroristen:**

  -> teweegbrengen van politiek-ideologische veranderingen door het creëren van angst.

  -> grote dreiging is er nog niet maar potentie groeit wel

  -> toch herhaaldelijke oproepen tot het voeren van digitale oorlog door ISIS

  -> groeperingen plaatsen info en instructievideo's om digitale vaardigheden van aanhangers verder te verspreiden

- **Cybervandalen en scriptkiddies:**

  -> beperkte dreiging voor organisaties

  - **Cybervandalen:**

    -> gevarieerd kennisniveau en voeren hacks uit om aan te tonen dat ze er toe in staat zijn.

  - **Scriptkiddies:**

    -> beperkte kennis

    -> handelen vanuit baldadigheid en het zoeken naar een uitdaging

    -> maken met opzet gebruik van een verwijzing naar ISIS, wordt gebruikt als misleiding of voor een choquerend effect vanwege de media-aandacht

- **Hacktivisten:**

  -> ideologische motieven of pattriotische hackers

  -> geopolitieke context en eerder eenvoudige digitale activiteiten

  -> neemt toe tijdens intra- en internationale conflicten, aanslagen en incidenten

- **Interne actoren:**

  -> individuen die in een organisatie aanwezig zijn of zijn geweest

  -> (ex-)medewerkers, inhuurkrachten en leveranciers

  -> naast financiële, politieke of persoonlijke motieven kunnen ook menselijke fouten aan de oorzaak liggen bij het aantasten van de betrouwbaarheid van een informatiesysteem

- **Cyberonderzoekers:**

  -> zoeken kwetsbaarheden in ICT-omgevingen om zwakke beveiliging aan de kaak te stellen

  -> gebruiken media om bevindingen te publiceren en de bewustwording over cybersecurity te vergroten

  -> onderzoekers of journalisten die kwetsbaarheden willen aantonen

  -> kwetsbaarheden op een verantwoordelijke manier melden

- **Private organisaties:**

  -> kunnen verantwoordelijkheid van informatiesystemen aantasten voor financieel gewin

  -> bedrijfsspionnage

  -> concurrentiepositie verbeteren

- DE BEDOELINGEN VAN DE DIVERSE ACTOREN

  -> BEROEPSCRIMINELEN : geldelijk gewin (direct of indirect)

  -> STATELIJKE ACTOREN : geopolitieke (of interne) machtpositie verbeteren

  -> TERRORISTEN : maatschappelijke verandering bewerkstelligen, bevolking vrees aanjagen

  -> CYBERVANDALEN EN SCRIPTKIDDIES : aantonen kwetsbaarheden, baldadigheid, uitdaging

  -> HACKTIVISTEN : ideologische motieven

  -> INTERNE ACTOREN : wraak, geldelijk gewin, ideologische motieven

  -> CYBERONDERZOEKERS : aantonen zwakheden, eigen profilering

  -> PRIVATE ORGANISATIES : verkrijging van waardevolle informatie

3.3 TOOLS: MALWARE & DIVERSE SOORTEN AANVALLEN

-> zijn geavanceerder geworden

-> meer kant-en-klare middelen

-> wordt professioneler

-> richt zich op meer verschillende systemen

3.3.1 ransomware

-> groeiend probleem en de hoeveelheid groeit verder

-> nieuwe varianten

-> opbrengsten die criminelen realiseren zijn hoog

-> bij nieuwere versies is het niet mogelijk om versleutelde bestanden terug te krijgen

-> aangewezen op back-ups

-> 100-700€ per gehackte computer betalen aan crimineel

-> nieuwe doelgroepen

-> naast versleutelen bestanden, ook sd-kaarten, USB-sticks en netwerkbronnen

- **Ransomweb:**

  -> via een kwetsbaarheid op webservers

  -> versleutelt ongemerkt informatie in de database

  -> ontsleutelt die pas weer op basis van geheime sleutel

  -> deze sleutel vaak opgeslagen op een server die de aanvaller host

  -> via e-mails uit de naam van microsoft

  -> preventie dmv back-ups

  -> mobiele platformen is nog beperkt (meestal aanvallen op android 96%)

  -> SaaS-achtige diensten voor het onderzoeken van netwerkfouten worden gebruikt

- **Mimikatz:**

  -> geschikt voor achterhalen paswoorden

  -> aanvallers gebruiken in sommige gevallen kant-en-klare exploits via metasploit

  -> niet alleen tools, ook exploits, exploitkits en malware

  -> **Exploit:** stukje software of hoeveelheid gegevens die gebruikmaakt van een bug, glitch of kwetsbaarheid in de software van een apparaat

  -> **RAT's:** vaker misbruikt voor digitale betaalfraude, staat voor 'Remote Acces Trojan'

  Zijn gemakkelijk te verkrijgen, digitale fraude wordt hierdoor laagdrempelig en toegankelijk voor verschillende dadergroepen.

3.3.2 denial of service aanvallen

-> anti-DDoS-maatregelen lijken meer en meer succesvol te zijn.

-> aanvallen blijven echter wel plaatsvinden

-> amplificatie is de methode die aanvallers hiervoor gebruiken: verstuur een klein verzoek en verwacht een groot antwoord

-> maken gebruik van UDP hierdoor kan gebruiker een IP adres opgeven waar het antwoord naar terug moet, uiteraard het aan te vallen adres.

-> door beperkte filtering van sommige netwerkbeheerders kunnen aanvallers een willekeurig IP-adres opgeven. Dan is er sprake van spoofing.

3.3.3 obfuscatie

-> proberen niet op te vallen en zo min mogelijk sporen na te laten.

-> moeilijk traceerbaar

-> opsporen verdacht verkeer bemoeilijkt door bonafide domeinnamen, websites en diensten voor communicatie door malware

-> door een TLS-versleuteling is niet inzichtelijk welke informatie een systeem binnen het netwerk uitwisselt.

-> malwareschrijvers vertroebelen hun malware om analyse door specialisten moeilijker te maken en soms doen ze dit ook juist niet wat het ontleden makkelijker maakt.

-> ontdekken van malware binnen een netwerk is echter moeilijk.

-> het voorkomen van herkenning is blijkbaar belangrijker dan het voorkomen van herkenning van de intenties en werkwijze

3.3.4 aanvalsvectoren

Dit zijn methoden die aanvallers gebruiken om hun slachtoffers aan te vallen. Aanvalsvector is het vehikel waarmee aanvaller probeert controle te krijgen over het systeem. Aanvallers combineren meestal meerdere aanvalsvectoren.

- **Phishing:**

  -> hét middel voor gerichte aanvallen

  -> emails lijken afkomstig van betrouwbare partijen.

  -> nadruk licht op het bedrijfsleven

  -> door het succes van spearphishing is deze vorm van social engineering de primaire aanvalsvector voor digitale spionage

- **Wateringhole-aanvallen:**

  -> aanvaller verspreidt zijn exploits en malware via een website die veel van zijn slachtoffers regelmatig bezoeken door misbruik te maken van een kwetsbaarheid in deze website

  -> daarna probeert de aanvaller meestal de systemen van bezoeker te infecteren via een exploit

- **Malvertising:**

  -> malvertising zijn verwerkt in heel veel websites, dit betreft een soort wateringhole-aanval

  -> specifieke groep van gebruikers zijn het doelwit.

  -> ze maken gebruik van real-time bidding advertentie netwerken.

- **JavaScript-bibliotheken:**

  -> bieden aanvallers veel potentie en is een interressant hulpmiddel

  -> aanvallers proberen een javascript-bibliotheek t emanipuleren.

  -> men kan vervolgens alle websites aanvallen die dynamisch gelinkt zijn met deze library

  -> grote groep gebruikers in korte tijd een enkel stuk malafide code aangeboden

- **Macro's:**

  -> dienen om virussen binnen een netwerk te verspreiden.

  -> wordt vooral toegepast om malware te downloaden en te installeren

  -> social engineering wordt gebruikt om de gebruiker alsnog de macro’s laten in te schakelen

- **Draadloze routers:**

  -> interressante hulpmiddelen voor aanvallers omdat deze routers op verschillende manieren zijn aan te vallen

  -> weinig gebruikers die de vereiste updates op deze routers installeren.

  -> kwetsbaarheden zijn gedurende langere tijd te misbruiken.

Overzichtschema doelwitten te vinden op pagina 62 cursus.