HODARI

Ontwikkelingen van informatiebeveiliging en privacy in de bouwwereld

R. (Ruud) Buurma en M.T.A. (Marcel) Klaver
Eindhoven
oktober 2021

OPENBAAR

Trends en ontwikkelingen in de bouwsector

1

1. Trends en ontwikkelingen in de bouwsector
2. Uit het nieuws
3. Principes cybersecurity
4. Aanvalsvectoren
5. Leveranciersmanagement
6. Ontwikkelingen AVG

Trends en ontwikkelingen in de bouwsector

Introductie

- **Robotisering**: Robots zullen een belangrijke rol gaan spelen, bijvoorbeeld bij het metselen van muren in een fabriek.
- **Drones**: Drones zijn goede middelen om moeilijk bereikbare plekken te controleren, zoals een brug of liftschacht.
- **BIM (Bouwwerk Informatie Model)**: Dit is een digitaal proces waardoor beter in het proces wordt samengewerkt en de faalkosten aanzienlijk worden teruggebracht.
- **VR (Virtual Reality) en AR (Augmented Reality)**: Op deze manier kunnen uitvoerders een blik werpen op een virtuele bouwplaats en daarnaast is het ook voor kopers mogelijk virtueel rond te lopen in hun toekomstige woning.
- **IoT (Internet of Things)**: IoT kan binnen de bouw worden gebruikt door sensoren te plaatsen in gebouwen. Ook kunnen bouwdelen uitgerust worden met chips zodat deze gevolgd kunnen worden.

Uit het nieuws

2

1. Trends en ontwikkelingen in de bouwsector
2. Uit het nieuws
3. Principes cybersecurity
4. Aanvalsvectoren
5. Leveranciersmanagement
6. Ontwikkelingen AVG

Uit het nieuws
Nieuwsberichten

- "Industrieconcern VDL Groep getroffen door digitale aanval", oktober 2021, NOS
- "Ondernemer toont zich behoorlijk laks bij cyberaanvallen" van Onderzoek van Ministerie Van Economische Zaken en Kamer van Koophandel, oktober 2021, Leidsch Dagblad
- "Politie waarschuwt voor spoofing met Nederlandse 06 nummers" zegt de politie tegen de Gelderlander, oktober 2021, Security.nl
- "Versterking aanpak cybercrime", 2021, Ministerie van Justitie en Veiligheid
- "Cyberrisico's zijn overal: ook in de bouw", oktober 2019, Nieuwsbrief Cobouw
- "Ondernemers niet goed voorbereid", Alert Online
- "Honderden Nederlandse beveiligingscamera's zijn onveilig", januari 2020, Pointer

Wat hierbij opvalt is het volgende:
- meer dan helft slachtoffers doet geen aangifte;
- kwart medewerkers geeft aan dat geen maatregelen zijn genomen;
- geslaagde hack kost gemiddeld EUR 67.000;
- Nederlandse bedrijven krijgen per week gemiddeld 294 cyberaanvallen te verduren;
- jaarlijks krijgt één op de vijf bedrijven met een hack te maken.

Principes cybersecurity

3

1. Trends en ontwikkelingen in de bouwsector
2. Uit het nieuws
3. Principes cybersecurity
4. Aanvalsvectoren
5. Leveranciersmanagement
6. Ontwikkelingen AVG

Principes cybersecurity
Wat is cybersecurity / informatiebeveiliging?

Het Nationaal Cyber Security Centrum (NCSC) omschrijft cybersecurity als volgt:

"Alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer. Ook worden maatregelen genomen om schade te beperken en/of te herstellen als die toch is ontstaan."

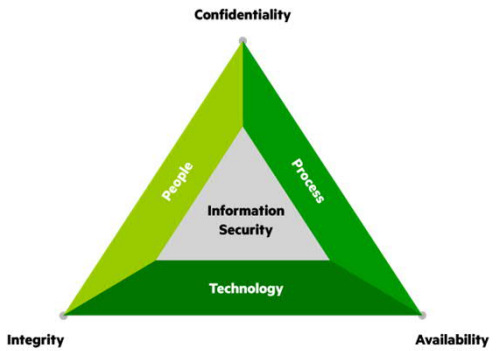
Schade in deze situatie erg breed:
- financiële schade;
- gegevensdiefstal;
- reputatieschade;
- productie- en omzetverlies;
- ontevreden medewerkers;
- overtredingen van de wet.

Principes cybersecurity
BIV en de vijf fases van cybersecurity

BIV (of CIA in het Engels) staat voor deze drie begrippen:
- **Beschikbaarheid** betekent dat informatie altijd beschikbaar is voor de juiste gebruikers.
- **Integriteit** betekent dat de informatie betrouwbaar, kloppend en volledig is. Ook mag de informatie niet onbewust of onrechtmatig gewijzigd of verwijderd worden.
- **Vertrouwelijkheid** betekent dat de informatie alleen is in te zien door geautoriseerde gebruikers.

Goede beveiliging bestaat uit verschillende soorten technische en organisatorische maatregelen gerelateerd aan mensen, processen en technologie.

Vijf fases van cybersecurity en hoe beveiligingsmaatregelen gecategoriseerd kunnen worden volgens NIST (National Institute of Standards):
- identificatie;
- bescherming;
- detectie;
- respons;
- herstel.



Principes cybersecurity
Continu verbeteren

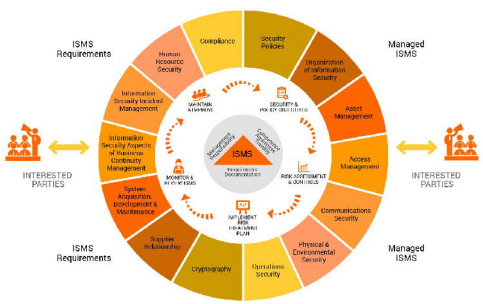
ISC2 hanteert binnen CISSP (Certified Information Systems Security Professional) de volgende domeinen:

- information security governance en risk management;
- access control;
- security architecture and design;
- physical and environmental security;
- telecommunications and network security;
- cryptography;
- business continuity and disaster recovery planning;
- legal, regulations & compliance;
- software development security;
- security operations;
- supplier security management.

Cybersecurity is geen eenmalige oefening, maar een proces van constante optimalisatie:

- ISMS (Information Security Management Systeem);
- plan-do-check-act (PDCA) cyclus.

CISSP® Certified Information Systems Security Professional

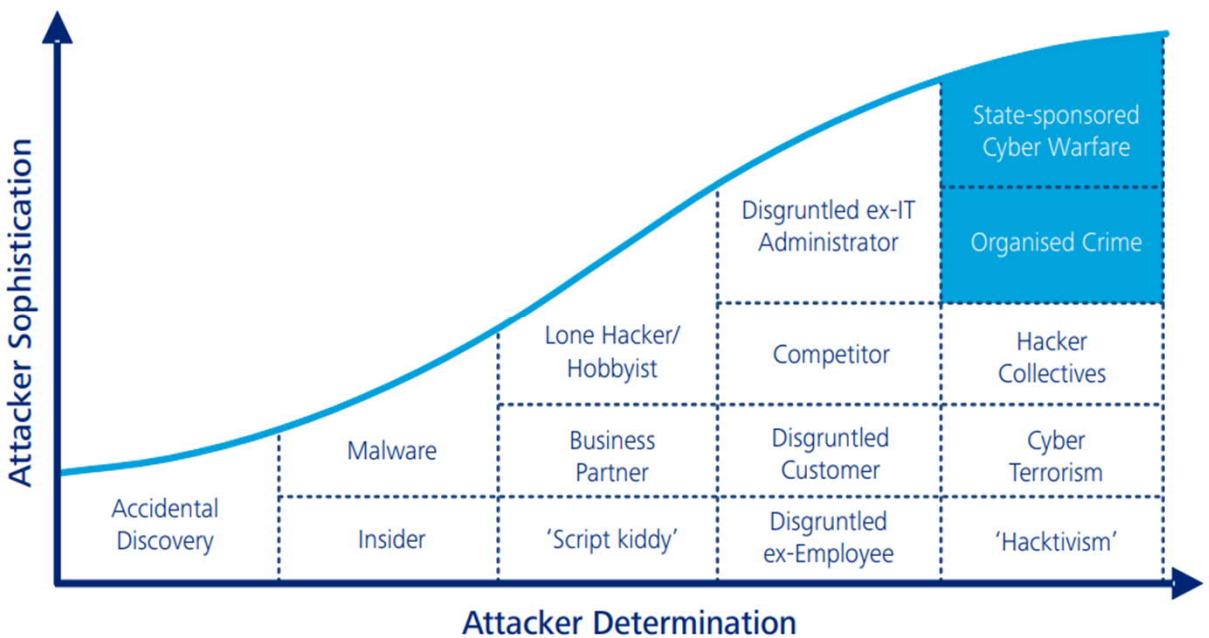


Aanvalsvectoren

4

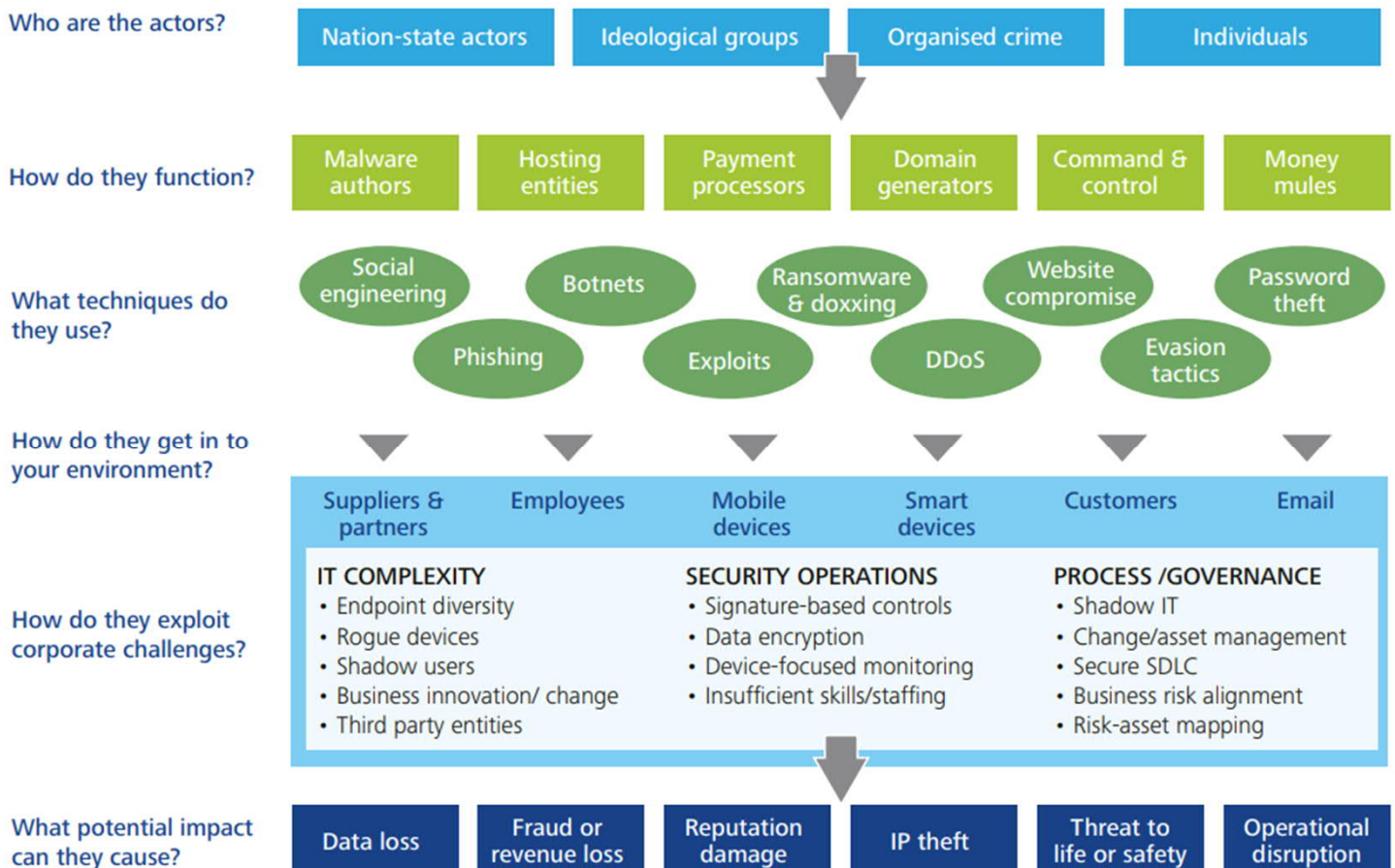
1. Trends en ontwikkelingen in de bouwsector
2. Uit het nieuws
3. Principes cybersecurity
4. Aanvalsvectoren
5. Leveranciersmanagement
6. Ontwikkelingen AVG

Aanvalsvectoren
Van script kiddie naar nation state

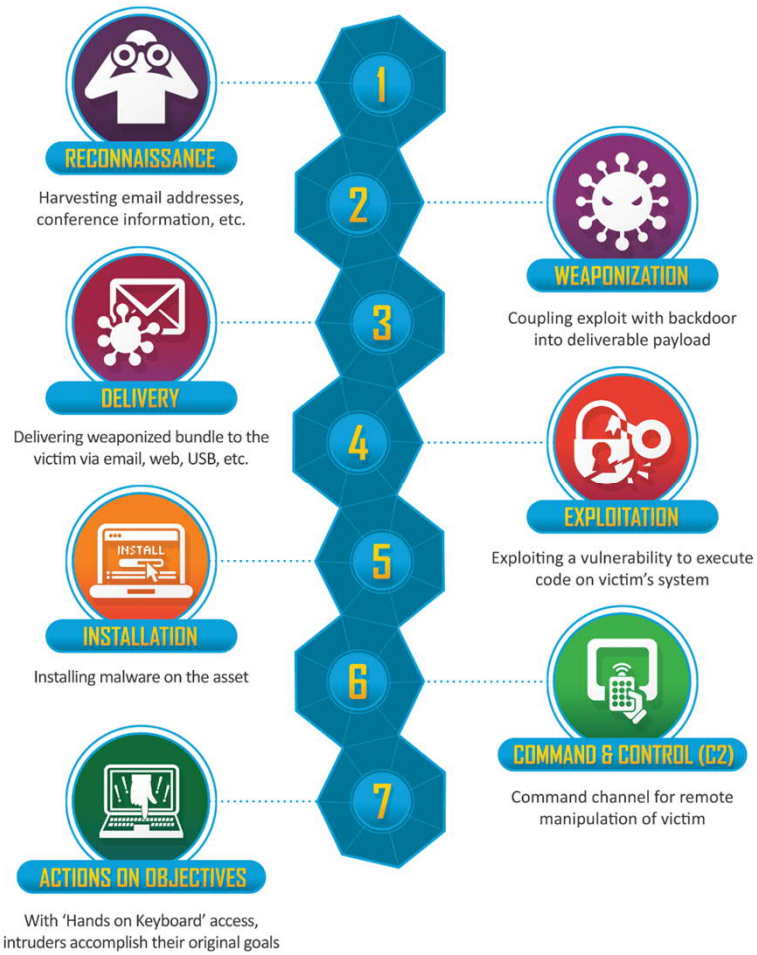


- Zelfs als script kiddie kun je gemakkelijk en goedkoop aan hacking tools en exploits/malware komen zoals Kali Linux.
- De wereld van cybercrime is geprofessionaliseerd en gecommercialiseerd.
- Op het darkweb is voor elke stap in de cyber kill chain een partij te vinden die hierin gespecialiseerd is.

Aanvalsvectoren
TTPs en aanvalsvectoren



Aanvalsvectoren
Cyber kill chain

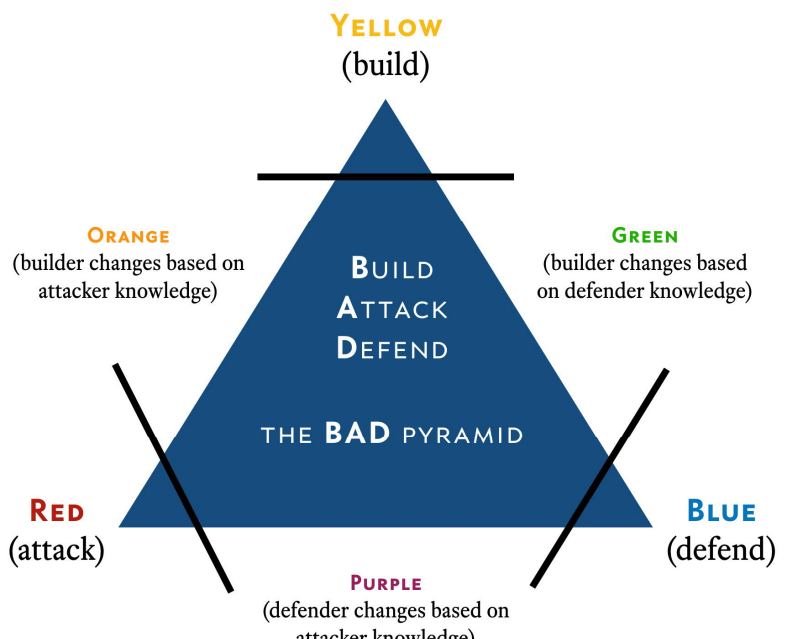


- Cyber kill chain framework is oorspronkelijk ontwikkeld door het CSIRT van Lockheed Martin.
- Meer dan 90% van de succesvolle hacks vinden plaats door een vorm van phishing (vaak e-mail).
- Grote 'nation states', zoals de VS, Rusland en China hebben over het algemeen slechts 20 minuten nodig om van fase 3 naar 6 te komen.
- Stap 1 en 3 focust zich vaak op de mens als zwakste schakel.
- Stap 4 misbruikt technische kwetsbaarheden op systemen.

Aanvalsvectoren
Technische aanvalsvectoren en kwetsbaarheden

- Aantal aanvalsvectoren:
  - malware;
  - man-in-the-middle attack;
  - ddos;
  - SQL injection;
  - zero-day exploit;
  - cross site scripting (XSS).
- Vulnerability management:
  - geautomatiseerd:
    - vulnerability scan;
    - policy compliance scan;
    - web application scan.
- Penetration testing:
  - start vaak met geautomatiseerde scans;
  - altijd manuele handeling door pentester om verder te komen.
- Pentesting versus red teaming.
- Red teaming versus blue teaming versus purple teaming.

MITRE ATT*CK model:



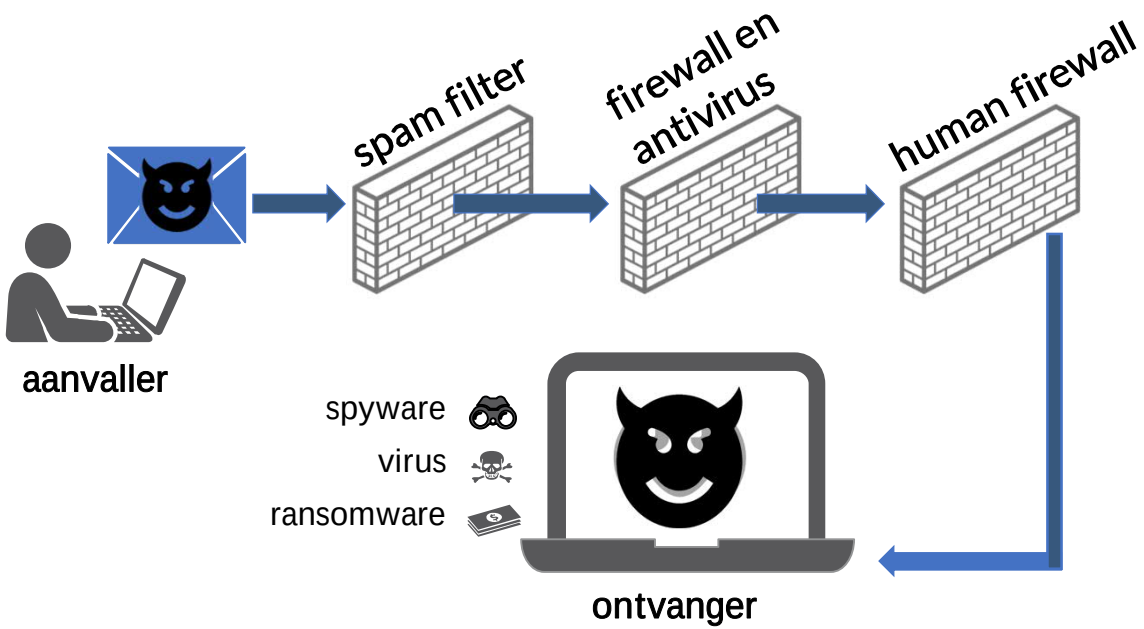
Aanvalsvectoren
Social engineering

- Bronnen voor hackers:
  - social media;
  - bedrijfswebsites;
  - verenigingen- en congressites;
  - publicaties en krantenartikelen;
  - foto's met metadata (EXIF);
  - darkweb:

- Social engineering:
  - Techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken (Wikipedia).
  - Werken met mystery guests.

- Doxing (of doxxing):
  - De handeling waarbij identificerende informatie over iemand online wordt onthuld, zoals zijn of haar echte naam, woonadres, werkplek, telefoon, financiële en andere persoonlijke informatie. Die informatie wordt dan openbaar gemaakt, zonder toestemming van het slachtoffer.

Aanvalsvectoren
Phishing: soorten ongewenste e-mails



Business e-mail compromise (BEC) wordt ook wel CEO-fraude genoemd.

Aanvalsvectoren
Herkennen en voorkomen van phishing mails

- **mensen:**
  - slecht geschreven (grammaticaal);
  - afzender van publiek domein (zoals bijvoorbeeld Gmail / Hotmail), gespoofd domein of verkeerd gespeld (typosquatting);
  - verdachte bijlagen of links in de mail;
  - zet aan tot actie;
  - gevoel van urgentie en tijdsdruk;
  - afzender wil geld of persoonlijke informatie zoals bankgegevens, wachtwoorden of informatie over organisatie(structuur) en medewerkers.

- **proces:**
  - beveiligingsbewuste cultuur top-down gedragen;
  - duidelijke procedures voor grote betalingen: vier-ogen-principe.

- **techniek:**
  - sender policy framework (SPF);
  - domainkeys indentified mail (DKIM);
  - domain-based message authentication, reporting and conformance (DMARC);
  - DNSSEC en DNS-over-HTTPS (DoH);
  - flags toevoegen wanneer de ‘sender’ en ‘return sender’ niet hetzelfde zijn;
  - spamfilters toepassen en up-to-date houden;
  - technische functiescheiding.

Voorkomen CEO-fraude:
- maak medewerkers attent op het bestaan van CEO-fraude;
- train medewerkers erop om niet te antwoorden op een e-mail (zeker wanneer het gevoelige informatie betreft), maar het e-mailadres te selecteren uit de contactenlijst van het bedrijf of de medewerker zelf;
- maak werknemers bewust van het feit dat een stem niet per se echt hoeft te zijn maar door criminelen kan zijn gemanipuleerd;
- laat werknemers na een telefonisch ontvangen verzoek een betaling te doen bellen met de veronderstelde leidinggevende via de intern bekende telefoonnummers;
- bekijk de website en profielen op social media van de organisatie en medewerkers kritisch; is het nodig de namen, functies en contactgegevens van medewerkers openbaar te maken?

Aanvalsvectoren

Man in the middle attack: openbare wifi en LAN

De makkelijkste manier om achter een wachtwoord te komen is om er naar te vragen in een nagemaakt scherm.

communicatie kan gemanipuleerd worden op onvertrouwde netwerken.

VPN op je bedrijfslaptop zorgt voor een veilige verbinding

https en bladwijzers kunnen je nog extra beschermen

Aanvalsvectoren

Toegangsbeveiliging: sterke versus zwakke wachtwoorden

- gebruik in plaatst van een wachtwoord een ‘wachtzin’ (‘passphrase’) (uniek, lang en moeilijk te raden);
- gebruik (vijf) verschillende wachtwoorden voor groepen accounts of een wachtwoordkluis;
- wijzig je wachtwoord regelmatig;
- pas MFA (multifactor authenticatie) toe:
  - wat je weet;
  - wat je hebt;
  - wat je bent.

Aanvalsvectoren
Supply chain attack: recente succesvolle aanvalsvector

- Recente aanvallen:
  - juli 2021: CVE-2021-30116 Zero-Days Used by REvil in Kaseya Ransomware Attack;
  - juli 2021: CVE-2021-35211 SolarWinds Serv-U Zero-Day Vulnerability;
  - maart 2021: iOS Developers Targeted by XcodeSpy, Trojanized Xcode Project.

- Supply chain attack:
  - Volgens MITRE ATT&CK raamwerk: methode om code, producten of mechanismen voor de levering van producten vóór ontvangst door een eindgebruiker te manipuleren met het oog op het beschadigen van data of systemen.
  - Volgens ENISA: Een combinatie van tenminste twee aanvallen, waarbij als eerste de leverancier aangevallen wordt en deze te gebruiken om een volgend doel aan te vallen en toegang te krijgen tot haar assets. Dit doel kan een andere leverancier of de uiteindelijke klant zijn.
  - Vaak grote terroristische groeperingen, criminele organisaties of nation states achter dit soort aanvallen.
  - Maakt misbruik van trusted relaties met leveranciers (vaak via patch servers).
  - De hele operatie (cyber kill chain) duurt vaak jaren.

Wat er tegen te doen:
- controleer je leveranciers op hun maatregelen (en certificeringen);
- zelf goed beveiliging en incident management inregelen;
- communiceer over incidenten met buitenwereld.

ATTACK TECHNIQUES USED TO COMPROMISE A SUPPLY CHAIN	
Malware Infection	e.g. spyware used to steal credentials from employees.
Social Engineering	e.g. phishing, fake applications, typo-squatting, Wi-Fi impersonation, convincing the supplier to do something.
Brute-Force Attack	e.g. guessing an SSH password, guessing a web login.
Exploiting Software Vulnerability	e.g. SQL injection or buffer overflow exploit in an application.
Exploiting Configuration Vulnerability	e.g. taking advantage of a configuration problem.
Physical Attack or Modification	e.g. modify hardware, physical intrusion.
Open-Source Intelligence (OSINT)	e.g. search online for credentials, API keys, usernames.
Counterfeiting	e.g. imitation of USB with malicious purposes.

Leveranciersmanagement

5

1. Trends en ontwikkelingen in de bouwsector
2. Uit het nieuws
3. Principes cybersecurity
4. Aanvalsvectoren
5. Leveranciersmanagement
6. Ontwikkelingen AVG

Leveranciersmanagement
Supplier security management: (SaaS) clouddiensten

- Hoe kun je een goede leverancier herkennen?
  - in bezit van certificeringen/verklaringen of onafhankelijke auditrapporten;
  - minimaal jaarlijkse pentesten;
  - gedegen beveiligingsfunctionaliteit in product zelf:
    - koppeling met eigen identity provider (en/of MFA);
    - (API koppelingen voor) directe monitoring en toegang tot audit logs.
  - gebruik van professionele hosting providers in bezit van alle nodige certificeringen.

- Welke belangrijke certificeringen/verklaringen zijn er:
  - ISO 9001 certificering (kwaliteitsmanagement);
  - ISO 27001 certificering;
  - ISO 27017 (in geval van cloud);
  - ISO 27018 (in geval van cloud en persoonsgegevens);
  - ISAE 3000 verklaring;
  - ISAE 3402 verklaring;
  - Cloud Security Alliance membership.

Punten die moeten worden beoordeeld:
- de scope van een certificering aan de hand van het SoA (statement of applicability);
- welke persoonsgegevens worden verwerkt;
- de verwerkersovereenkomst;
- afspraken omtrent de uitwisseling met derde landen volgens de nieuwe SCC (standard contract clausules) (juli 2021), wanneer persoonsgegevens buiten de EER worden uitgewisseld;
- locaties waarvandaan toegang tot de gegevens kan worden verkregen;
- bij faillissement van de leverancier moet de dienst door kunnen draaien.

Ontwikkelingen AVG

6

1. Trends en ontwikkelingen in de bouwsector
2. Uit het nieuws
3. Principes cybersecurity
4. Aanvalsvectoren
5. Leveranciersmanagement
6. Ontwikkelingen AVG

Ontwikkelingen AVG
Eisen ten aanzien informatiebeveiliging: wet- en regelgeving

Eisen die aan informatiebeveiliging worden gesteld:

- voldoen aan informatiebeveiliging was al eerder verwoord in andere wet- en regelgeving;
- Wet bescherming persoonsgegevens met de meldplicht datalekken, die inmiddels is vervallen;
- Wet bescherming bedrijfsgeheimen, bedrijfsgeheimen (waaronder veelal persoonsgegevens) beschermen;
- in Burgerlijk Wetboek wordt in artikel 2:393 verwezen naar de "betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking" in het kader van het onderzoek door een accountant naar de jaarrekening;
- veel organisaties werken aan certificering om hun informatiebeveiliging aan te tonen: bijvoorbeeld ISO 27001;
- de AVG schrijft in artikel 24, 25, 27 en 28 "technische en organisatorische maatregelen" voor.

Ontwikkelingen AVG
Activiteiten van de Autoriteit Persoonsgegevens

Enkele cijfers over het jaar 2020 met betrekking tot de activiteiten van de Autoriteit Persoonsgegevens:

- ruim 24.000 datalekken ontvangen;
- bijna 26.000 klachten ontvangen, veel over de inzage persoonsgegevens;
- circa 60 onderzoeken verricht;
- 7 boetes opgelegd voor ruim 2 miljoen euro;
- 120 wetgevingsadviezen verleend;
- circa 6.000 informatieverzoeken afgehandeld.

De Autoriteit Persoonsgegevens heeft controles uitgevoerd bij meer dan 400 overheidsorganisaties, bijna 100 ziekenhuizen en ruim 30 zorgverzekeraars.

Zij heeft onderzoeken gedaan over:

- rapport Smartcities;
- boete wifi tracking;
- onderzoek online (video) bellen;
- onderzoek corona-apps;
- onderzoek naar TikTok;
- visie op toezicht AI en algoritmes.

Ontwikkelingen AVG
Smartcities

Uit rapport onderzoek naar Smartcities komt het volgende naar voren naar aanleiding van onderzoek bij 12 gemeenten:

- Definitie Smartcity: verzamelen en verwerken van (persoons) gegevens over of in de openbare ruimte door inzet van sensoren, technologie of andere toepassingen.
- Toepassingen: wifi- en bluetooth-tracking, inzet van camera's, sensoren die data verzamelen over verkeer of geluid.

Aanbevelingen uit het rapport zijn:

- bepalen rechtmatigheid, concrete doelstelling, alternatieven;
- DPIA uitvoeren, tijdig actualiseren, publiceren, betrokkenen meenemen, anonimiteit;
- beleid opstellen met betrekking tot Smartcities;
- bouw een privacy organisatie, mensen, middelen;
- programma van eisen bij aanbesteding.

Een DPIA is verplicht bij:

- grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens;
- bij delen van persoonsgegevens met andere (private) partijen;
- grootschalige verwerkingen en/of stelselmatige monitoring van openbaar toegankelijke ruimen met camera's, webcams of drones;
- grootschalig en/of systematisch gebruik van flexibel cameratoezicht;
- grootschalige verwerkingen en/of stelselmatige monitoring van locatiegegevens.

Ontwikkelingen AVG
Tips voor privacy

Hieronder volgen enkele tips om de privacy binnen organisaties te vergroten:

- vraag niet meer gegevens van de klant dan noodzakelijk;
- sla gegevens van je klanten veilig op;
- verspreid de gegevens van je klanten niet zonder toestemming van de klant;
- zorg dat je altijd op papier hebt staan met wie je klantgegevens deelt en hoe daarmee omgegaan wordt;
- een klant mag je verzoeken zijn gegevens te verwijderen of aan te passen;
- geef aan waar je de gegevens van de klanten bewaart en hoe lang;
- geef aan wie er toegang heeft tot de gegevens van de klant.

Ontwikkelingen AVG
Tips voor informatiebeveiliging

Hieronder volgen enkele tips om de informatiebeveiliging binnen organisaties te vergroten:

- creëer bewustzijn;
- breng informatiestromen binnen de onderneming (incl. communicatie via website) in kaart;
- stel het vereiste niveau van bescherming vast;
- regel de monitoring van de informatiestromen;
- weet welke medewerkers toegang hebben (gehad);
- wie is binnen of buiten de onderneming verantwoordelijk voor informatiebeveiliging;
- zorg voor gescheiden bevoegdheden en rechten;
- zorg ervoor dat de rechten worden gewijzigd zodra de functie van een medewerker verandert of hij uit dienst treedt;
- maak afspraken met medewerkers onder welke voorwaarden eigen devices worden gebruikt;
- stel vast hoe wordt omgegaan met de risico's van verlies, vernietiging en vervalsing van belangrijke informatie;
- stel een noodplan op voor het geval zich infrastructurele verstoringen voordoen;
- werk uitsluitend met originele hardware en software;
- zorg voor een werkend back-up beleid en procedure;
- leg vast hoe digitale informatiedragers na gebruik worden vernietigd;
- stel vast hoe applicaties worden beschermd door middel van toegangscontroles, zoals gebruikersnamen en wachtwoorden;

Ontwikkelingen AVG
Tips voor informatiebeveiliging

- zorg voor een adequate bescherming door gebruik van beschermingssoftware, firewalls;
- stel vast welke verbindingen de onderneming heeft met externe systemen en netwerken en dat deze adequaat zijn beveiligd;
- zet beleid en procedures op rondom beveiliging van data;
- stel vast welke informatiestromen essentieel zijn voor het functioneren en voortbestaan van de organisatie;
- zorg voor een helder en compleet identity en access proces;
- maak afspraken voor het installeren van nieuwe software of apps;
- stel een BCP (business continuity plan) op waarin is vastgelegd welke acties moeten worden uitgevoerd in geval van een calamiteit;
- stel een procedures op voor het gebruik van verwijderbare media, zoals USB-sticks, externe harde schijven,.

Ontwikkelingen AVG
Tips voor informatiebeveiliging

- Is vastgelegd dat alle medewerkers eigen gebruikersnamen en wachtwoorden hebben en/of Is vastgelegd dat medewerkers de verplichting hebben om persoonlijke wachtwoorden geheim te houden. Werken met *two factor authentication.*
- Is er antivirussoftware in gebruik welke regelmatig gecontroleerd en geüpdatet wordt? Zijn er firewalls in gebruik en wordt regelmatig gecontroleerd of deze functioneren?
- Gebruiken bezoekers of klanten wifi faciliteiten binnen de onderneming of is een separaat gasten netwerk aangelegd?
- Maken de mobiele devices automatisch verbinding met openbare wifi hotspots? Wordt gebruikgemaakt van encryptie bij de uitwisseling van data via een extern wifi netwerk?

HODARI
PRIVACY COMPLIANCE SECURITY GOVERNANCE

HODARI provides services regarding privacy, compliance, information security and governance. We improve IT by reducing risks in information security and we help organisations to become in control. We offer high-quality solutions where even the most complex issues are solved in detail. We have gained extensive experience in various industries, such as the financial sector, energy sector, (central) government, legal profession, IT service providers and retail. We regularly act in projects related to mergers and acquisitions, reorganisations, findings of accountants or comments of supervisors.

HODARI bijvoorbeeld

071-2032385
hodari.nl

L. (Lodewijk) Benjaminse
lodewijk.benjaminse@hodari.nl
06-53736105