Henning Mortensen 31. aug. 21

Risikovurdering i en GDPR-kontekst

- En praktisk tilgang

Om underviseren

Uddannelse

- Cand. Scient. Pol., BA Oecon, Enkeltfag på ITU og Ålborg Universitet, Exam ESL, CIPP/E, CIPM, CIPT, FIP

Job

- CISO/CPO, Brødrene A&O Johansen
- Privacy evangelist, Wired Relations
- Formand for Rådet for Digital Sikkerhed
- Medlem af Datarådet
- Medlem af Cybersikkerhedsrådet
- Medlem af Virksomhedsforum for Digital Sikkerhed
- Underviser og foredragsholder

Historik

- Chefkonsulent i DI i mere end 15 år med informationssikkerhed og personoplysninger som speciale
- Medlem af en række sikkerhedsråd under videnskabsministeriet
- Medstifter af Rådet for Digital Sikkerhed
- Tidligere bestyrelsesmedlem i ESL-foreningen, ISACA Danmark, m.fl.
- Har redigeret og/eller forfattet en lang række vejledninger om informationssikkerhed og beskyttelse af personoplysninger
- Modtager af Databeskyttelsesprisen 2018

LinkedIn

https://www.linkedin.com/in/henning-mortensen-343b0/ (connect gerne)

Henning Mortensen 31. aug. 21

Risikovurdering homo digitalis

Hvad er jeg bange for?	Hvorfor?	Hvad vil jeg gøre ved det?
Statens dataophobning	DNA i genom centeret kan anvendes til at straffe mine børnebørn i en kommende politisk virkelighed Fremtidig kloning af mig	Undgå at få taget vævsprøver i Danmark og i stedet benytte mig at udenlandske sundhedsudbyder og indkøb af udenlandsk medicin online
Statslig masseovervågning	Med ANPG i miljøzoner kortlægger staten når jeg kører ind og ud af de største byer Med første udkast til corona-app ved staten ved hvem jeg er i nærheden af	Tag toget, en taxa eller cyklen Undlade at installere app'en og brug TOR og Cubes
Kommerciel profilering	Private kommercielle aktører kender mine præferencer bedre end mig selv og kan manipulere med mig ud fra højestbydendes formål	Installer add-blockers og brug evt. privacy-venlige browsere
Arbejdsgivers overvågning	Arbejdsgiver har adgang til mine private oplysninger: kan se mine kreditkortoplysninger, når jeg køber ind, mine bankoplysninger når jeg omlægger lån og dialogen med min fagforening	Undlad at bruge mit arbejdsudstyr til private formål
Far og mor	Kan se når jeg søger information hos Enhedslisten, at jeg var i biografen i stedet for lektiecafe og besøgte boyfriend.dk, fordi jeg skal teste min seksualitet	Brug privacy-venlige browsere (uden historik) og VPN og undlad at installere visse apps
Hackere	Vil afpresse mig gennem ransomware, bruge min regnekapacitet, stjæle adgang til mine betalingstjenester og sælge mine oplysninger	Opdater, sikkerhedspakke, lange password/passwordhusker, ingen nøgenbilleder

Aktuelle trusler - statistik

DK CERTs trendrapport 2019 fra juni 2020

- Phishing, smishing, vishing
- Ransomware
- Onlinesvindel, fupbutikker
- Datalækager
- Sikkerhedsproblemer i CMS
- Malware
- APT-angreb på kritisk infrastruktur

Kilde: https://www.cert.dk/sites/default/files/uploads/PDF/DKCERT_Trendrapport_2020.pdf

Ransomware
Tre-trins afpresning

Kombination af ransomware-attack og supply-chain-attack

1. Stjæl organisationens data og afpres
2. Krypter og afpres
3. Afpres kunderne (og få dem til at lægge pres på organisationen)

Case: Den finske Vastaamo klinik

- Truer klinikken (£403.000)
- Truer patienterne med at offentliggøre deres journaler (€200-500)

Et hav af ofre og varianter:

- Ryuk, Maze, REvil, Lockbit og DearCry
- Internationalt: JBS (verdens største slagterivirksomhed), Colonial Pipeline Co. og Kaseya Ltd (med Coop som afledt offer),
- I Danmark: AK Techotel, Bauhaus, ISS, Demant og Norsk Hydro.

WIRED SUBSCRIBE NEWSLETTERS

WILLIAM RALSTON SECURITY 09.12.2020 06:00 AM

A dying man, a therapist and the ransom raid that shook the world

Patients put their trust in a therapy company to keep their notes and diagnoses private. Then the ransom demands arrived

GETTY IMAGES / WIRED

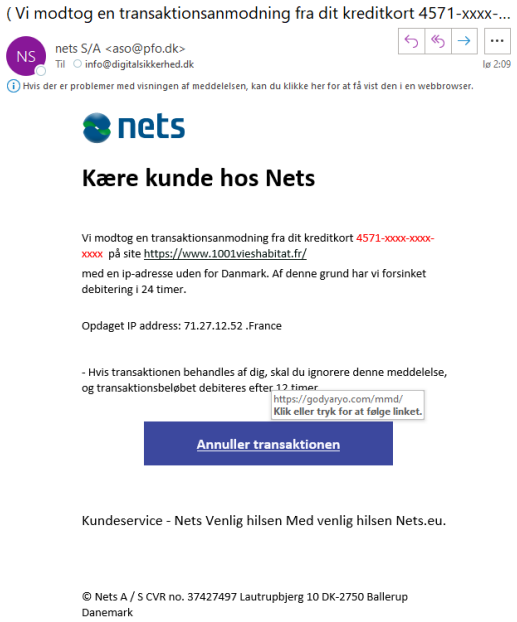
Jukka-Pekka Puro will never forget 2017. Facing the heartbreak of a divorce, Puro, a university lecturer in Turku, southwestern Finland, found himself tussling with depression. This spiralled into suicidal

Phishing

Arter af Phishing

Spear-phishing

- Angreb på en person med særlig betydning i en organisation: leder eller administrator


(Vi modtog en transaktionsanmodning fra dit kreditkort 4571-xxxx-...

NS nets S/A <aso@pfo.dk>
Til info@digitalsikkerhed.dk
lø 2:09

Hvis der er problemer med visningen af meddelelsen, kan du klikke her for at få vist den i en webbrowser.

nets

Kære kunde hos Nets

Vi modtog en transaktionsanmodning fra dit kreditkort 4571-xxxx-xxxx-xxxx på site https://www.1001vieshabitat.fr/
med en ip-adresse uden for Danmark. Af denne grund har vi forsinket debitering i 24 timer.

Opdaget IP address: 71.27.12.52 .France

- Hvis transaktionen behandles af dig, skal du ignorere denne meddelelse, og transaktionsbeløbet debiteres efter 12 timer.

https://godyaryo.com/mmd/
Klik eller tryk for at følge linket.

Annuller transaktionen

Kundeservice - Nets Venlig hilsen Med venlig hilsen Nets.eu.

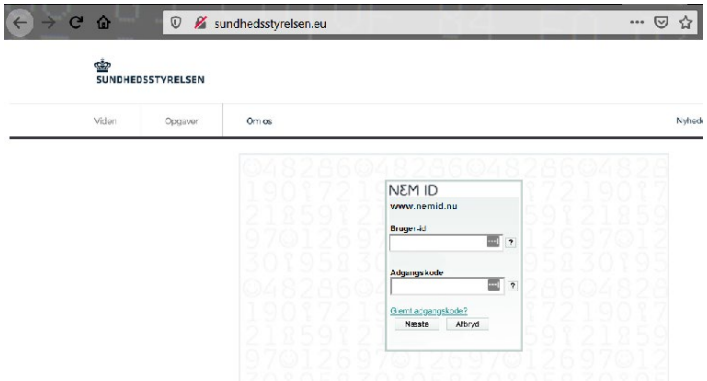
© Nets A / S CVR no. 37427497 Lautrupbjerg 10 DK-2750 Ballerup Danemark

Smishing

- Phishing via sms, så din telefon bliver kompromitteret
- Du bliver bedt om at klikke på et link i en sms

Vhishing

- Phishing via voice
- Brugeren bliver bedt om at lave et telefonopkald til et site, hvor man f.eks. skal indtaste kreditkortoplysninger eller bliver bedt telefonisk om at afgive kreditkortoplysninger, brugernavn/password eller andre brugeroplysninger mundtligt




Sundhedsstyrelsen har sendt dig ny Digital Post. Log på og læs den på sundhedsstyrelsen.net.

Med venlig hilsen
Digital Post fra det offentlige


Statens Serum Institut har sendt dig ny post. Log på og læs den på coronaprøver.net

Off-topic: Hvordan genkendes phishing?

Huskeregler for at undgå at klikke på phishing (på arbejde og derhjemme)

Vær skeptisk

- Vær altid skeptisk, når nogen forsøger at få dig til at klikke på et link
- Vær altid skeptisk, når nogen beder dig om oplysninger
- Hvis noget er for godt til at være sandt, er det formodentlig et forsøg på at svindle
- En kort tidsfrist til at gøre noget, bør få dig til at være skeptisk
- Er der mangelfulde informationer, så du først får detaljer, når du har klikket, bør du være skeptisk

Test mailen uden at klikke

- Tjek om afsenderens mail-adresse er en du kender
- Prøv at klikke på reply og se om den samme mailadresse kommer frem
- Hold musen hen over et link for at afsløre, hvor det vil tage dig hen (det kan være et andet sted end linket indikerer)

Tjek sproget

- Er sproget formfuldendt
- Er sproget i den stil du plejer at modtage
- Plejer du at modtage mails på engelsk

Tast i stedet for at klikke hvis muligt

- Indtast URL i browser i stedet for at klikke på link
- Tjek at hjemmesider begynder med https i stedet for http

Skift kommunikationskanal og søg bekræftelse

- Hvis du er i tvivl så ring til afsenderen

Brug unikke passwords og slå to-faktor autentifikation til

- Så du sikrer, at du ikke får din identitet brugt til et phishing angreb

Aktuelle trusler - hændelser

Storytelling

- Aflytning/overvågning: PRISM, UPSTREM, osv.
- Telefoni: tracking af soldater og demonstranter
- App-sikkerhed: tracking af lokation, norsk medie, efterretningstjenester + Cambridge Analytica
- IoT-sikkerhed: legetøj, voksenlegetøj
- IT-kriminelle: hacking, alle har salgsværdige data, CEO-fraud, ransomware
- Insidere: salg af data, med til ny arbejdsgiver
- Forensic linguistics: meget tekst kan spores
- Profilering: bidrag til kommerciel eller statssponseret profilering
- Fejl: upload til CMS, SSI

Trusselsaktører

Trusselsaktører

- Fremmede lande
- Kriminelle
- Idealister
- Psykopater
- Os selv - fejl

Risikovurdering i GDPR-kontekst

Udgangspunkt: behandling af personoplysninger udsætter den registrerede for risici. Der er mange steder i forordning, hvor aktiviteter afhænger af en vurdering af risici, f.eks.:

- Når den dataansvarlige skal iværksætte alskens tiltag
- Når det skal besluttes hvilke tiltag, der skal designes ind i en løsning
- Når SME skal beslutte om de skal dokumentere deres behandlingsaktiviteter
- Når det skal besluttes hvilke sikkerhedstiltag, der skal implementeres
- Når det skal besluttes om der skal rapporteres hændelser til tilsynsmyndighed og den registrerede
- Når det skal besluttes om der skal laves DPIA
- Når det skal besluttes om tilsynsmyndighed skal konsulteres før behandling iværksættes
- Obligatorisk aktivitet for DPO

Summa sumarum: Risikovurdering har fået en fremtrædende plads i forordningen

Risikovurdering og GDPR

Afdramatiserende bemærkninger

- Der er mange steder henvisning til vurdering af risiko
- Der er ingen formkrav
- Der er krav om risiko skal ses fra den registreredes perspektiv
- Genstanden for risikoen er ikke fastlagt: behandlingsaktivitet vs. informationsaktiv vs. hardware/software
- Risikovurderingens dybde er ikke fastlagt
  - Mavefornemmelse (følsomhed, trusselsbillede, mængde, brand, samfundskritikalitet,…)
  - Alle behandlingsaktiviteter
  - Alle systemer
  - Måle på tilgængelighed, fortrolighed, integritet, o.a.

- I har domæneviden, det har Datatilsynet ikke

Trusler: OCTAVE

Menneskelige trusler

- Tekniske midler
  - Insidere
    - Med forsæt
    - Uden forsæt
  - Eksterne
    - Med forsæt
    - Uden forsæt
- Fysiske midler
  - Insidere
    - Med forsæt
    - Uden forsæt
  - Eksterne
    - Med forsæt
    - Uden forsæt

Tekniske problemer

- Software
- Systemer
- Hardware
- Ondsindet kode

Trusler udenfor organisationens kontrol

- Strøm
- Telekommunikation
- Tredjeparter
- Naturkatastrofer

https://www.cert.org/resilience/products-services/octave/index.cfm

Trusler: ENISA

Grupper

- Jura
- Forbrydere
- Opsnapning og aflytning
- Udfald
- Fysiske angreb
- Uheld gennem handlinger
- Katastrofer
- Tab af aktiver
- Ikke korrekt virkemåde

Threat number	High Level Threats	Threats	Threat details	Exploit
1	Physical attack (deliberate/ intentional)			
2		*Fraud*		
3			Fraud by employees	
4		*Sabotage*		
5		*Vandalism*		
6		*Theft (devices, storage media and documents)*		
7			Theft of mobile devices (smartphones/ tablets)	
8			Theft of fixed hardware	
9			Theft of documents	
10			Theft of backups	
11		*Information leakage/sharing*		
12		*Unauthorized physical access / Unauthorised entry to premises*		
13		*Coercion, extortion or corruption*		
14		*Damage from the warfare*		
15		*Terrorists attack*		
16	Unintentional damage / loss of information or IT assets			
17				

Kilde: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

Trusler: Mitre

MITRE | ATT&CK®

Matrices Tactics Techniques Mitigations Groups Software Resources Blog Contribute Search

ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation
	Launchctl	Component Object Model Hijacking	File System Permissions Weakness	Control Panel Items	Kerberoasting	Query Registry	Shared Webroot	Video Capture	Multiband Communication		Service Stop
	Local Job Scheduling	Create Account	Hooking	DCShadow	Keychain	Remote System Discovery	SSH Hijacking		Multilayer Encryption		Stored Data Manipulation
	LSASS Driver	DLL Search Order Hijacking	Image File Execution Options Injection	Deobfuscate/Decode Files or Information	LLMNR/NBT-NS Poisoning and Relay	Security Software Discovery	Taint Shared Content		Port Knocking		System Shutdown/Reboot
	Mshta	Dylib Hijacking	Launch Daemon	Disabling Security Tools	Network Sniffing	Software Discovery	Third-party Software		Remote Access Tools		Transmitted Data Manipulation
	PowerShell	Emond	New Service	DLL Search Order Hijacking	Password Filter DLL	System Information Discovery	Windows Admin Shares		Remote File Copy		

Kilde: https://attack.mitre.org/

Trusler: Soloves trussels taxonomi

Informationsindsamling

- Surveillance: betragte, lytte, optage
- Interrogation: udspørge

Informationsbehandling

- Aggregation: kombinere data om en person
- Identification: linke data til et individ
- Insecurity: uautoriseret adgang og lækager
- Secondary use: formålsforskydning
- Exclusion: uigennemsigtig anvendelse

Informationsspredning

- Breach of confidentiality: information er ikke længere fortrolig og tillid er brudt
- Disclosure: afsløring af information, som fører til fordømmelse
- Exposure: udstilling af krop, sorg, m.v.
- Increased accessibility: forstærke adgangen til information
- Blackmail: trussel om at offentliggøre information
- Appropriation: misbrug af identitet til egen vinding
- Distortion: spredning af misledende information om individ

Invasion

- Intrusion: forstyrrer retten til at være alene
- Decisional interference: myndigheders indgriben i individernes private beslutninger

Kritik

- Taxonomien er på et højere abstraktionsniveau
- Mindre operationel
- Mindre relateret til en konkret hændelse

Trusler: Soloves trussels taxonomi

Eksempler:

Informationsspredning, exposure
Spredning af nøgenbilleder fra ekskærester
Kilde: https://www.dr.dk/nyheder/indland/en-mand-bag-en-skaerm-stjal-min-ret-til-bestemme-hvem-der-skal-se-mig-noegen

Informationssprednig, breach of confidentiality
SSI sender ved fejl danskernes sundhedsoplysninger til Kinesiske myndigheder
Kilde: https://www.version2.dk/artikel/anbefalet-brev-gik-galt-ukrypterede-cder-med-sundhedsdata-havnede-hos-kinas-visumkontor

Informationsindsamling, surveillance
Masseovervågning som f.eks. Afsløret af Snowden
Kilde: https://www.dr.dk/nyheder/viden/tech/snowdens-kaempelaek-afsloerede-usas-massive-overvaagning

Informationsbehandling, exclusion (uigennemsigtig anvendelse)
Restmateriale fra corona-test gemmes i Danmarks Nationale Biobank
Kilde: https://www.version2.dk/artikel/statens-serum-institut-glemte-at-fortaelle-biologisk-materiale-med-dna-corona-test-gemmes

Informationsbehandling, identification (linke data til individ)
Såbarheder kan udnyttes til at eksponere brugerdata
Kilde: https://www.comparitech.com/blog/information-security/firebase-misconfiguration-report/#What_data_is_exposed

Være generelt opmærksom på "ny teknologi"

- Det er ikke kun ondsindede aktører eller uvidende medarbejdere der er problemet
- Manglende viden forståelse af hvad ny teknologi kan udgør en stor trussel

Eksempler

- Bagdør for at servicere produkt
- Databehandlers selvstændige behandling
- Manglende oplysning om at produktet ringer hjem
- …

Risikovurdering: onPrem vs cloud

Eksempler på spørgsmål som bør overvejes i forbindelse med risikovurdering af cloud:

- **Uklar ansvarsfordeling ift. etablering af de korrekte arbejdsgange i cloudtjenester**
- **Uklarheder/manglende træning ift. hvordan cloudtjenester bruges, og dokumenter deles med uautoriserede**
- **Adgang til data udenfor EU - 24/7 support og underdatabehandlere**
- **Indsamling af diagnostiske data (i hvilket omfang ønsker organisationen at dele disse data)**
- **Monitorering af ændringer i service- eller aftalevilkår eller konfigurationer**

Harmonisering af trusselsmål

Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

Konsekvenser	*Kategori*	*Eksempel*
5	Væsentlige fysiske konsekvenser	• Der kan ikke leveres livsvigtig medicin til borgerne og det kan have fatale konsekvenser. • Borgerens liv er i fare, f.eks. ved afsløring af hemmelige adresser for voldsofre eller vidner. • Redningstransport kan ikke iværksættes. • Borgeren må forlade sit hjem.
4	Væsentlige økonomiske eller omdømmemæssige konsekvenser	• Borgeren kan ikke få udbetalt sine ydelser. • Borgeren er afskåret fra at gennemføre økonomiske transaktioner. • Borgerens forbrugspræferencer og psykologiske profil bliver gennemsigtige og udbudt til højestbydende på markedet. • Borgeren kan blive udstillet eller marginaliseret i sit sociale nærmiljø - herunder med betydelig skade på omdømme. Det kan f.eks. ved underretning om familie med omsorgssvigt eller indtagelse af stoffer.
3	Væsentlige IT-sikkerheds-mæssige eller sociale konsekvenser	• Uvedkommende adgang til væsentlige følsomme eller fortrolige oplysninger, f.eks. terminale, seksuelle eller psykiske sygdomme, misbrug af børn, vold i hjemmet eller religiøst betinget adfærd. • Uvedkommende adgang til oplysninger der kan anvendes til identitetstyveri. • Følsomme oplysninger om børn (f.eks. oplysninger om udadreagerende adfærd, vægtproblemer, mobning, læsevanskeligheder eller konflikter med andre børn) videregivet til klassekammerater eller deres forældre
2	Mindre økonomiske, IT-sikkerhedsmæssige eller sociale konsekvenser	• Borgeren kan ikke få et pas til en bestilt og betalt rejse. • Borgeren kan miste kontrol med login til et system eller få login eksponeret for uvedkommende.
1	Ubehag og reduktion af tilliden til digitaliseringen	• Konsekvenserne er – hvor ubehagelige de end er – afgrænset til et psykisk ubehag for den registrerede selv og uden, at der er fysiske, økonomiske eller sociale konsekvenser.
0	Ingen konsekvens	• Ingen konsekvens

Tre forståelser af risikovurdering

Risikovurdering

- Sandsynlighed og konsekvens
- Risiko set fra organisationens perspektiv: Det handler om risikoappetit
- Omfatter andet og mere end personoplysninger – f.eks. IPR, forretningsstrategi og forretningshemmeligheder
- ISO2700x-tilgangen

Vurdering af risiko for den registrerede

- Risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (artikel 32 og Datatilsynets sikkerhedsvejledning side 7): Det handler om beskyttelse af fundamental rettighed

Konsekvensanalyse

- Analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (artikel 35)

Risikovurdering

Husk at dokumenterer HVORFOR du ender på en bestemt konsekvens eller sandsynlighed. Det gør det lettere at validere og gentage analysen.

Konsekvens / Sandsynlighed	Lav	Mellem	Høj
Lav			
Mellem			
Høj			

Tool: Skabelon til risikovurdering

Excel-skabelon hos sikkerdigital.dk

				Risikovurdering					Risikohåndtering				
ID	Risiko - Hvad kan påvirke fortrolighed, tilgængelighed eller	Risiko ejer	Hvorfor er dette en trussel/risiko?	Skøn for Konsekvens	Hvorfor vurderes Konsekvensen til dette?	Skøn for Sansynlighed	Hvorfor vurderes sandsynligheden til dette?	Beregnet risiko	Acceptere et	Nye foranstaltninger	Konsekvens efter nye foranstaltninger	Ny sansynlighed	Ny restrisiko	Restrisiko Accepteret
1														
2	Insider tyveri	XXX	Fortrolighed	2	Målrettet	3	Kun politikker	6	Undgå	SIEM, Shadow IT	2	2	4	Accepteres
3	Fejl upload til CMS	XXX	Fortrolighed	4	Få men ofte følsomme	4	Set før	16	Undgå	DLP	3	2	6	Accepteres
4	Fejludsendelse af bilag	XXX	Fortrolighed	3	Få og følsomhed forskellig	4	Set jævnligt	12	Undgå	DLP, autofuldførelse	3	1	3	Accepteres
5	Hack af ESDH	XXX	Fortrolighed	4	Stor konsekvens for mange	2	Eksisterende foranstaltninger	8	Undgå	Pseudonymisering	2	2	4	Accepteres
7								0					0	
8								0					0	
9	Hack af ESDH	XXX	Fortrolighed	4	Stor konsekvens for mange	2	Eksisterende foranstaltninger	8	Undgå	Pseudonymisering	2	2	4	Accepteres
10	Hack af ESDH	XXX	Integritet	5	Stor konsekvens for mange	1	Eksisterende foranstaltninger	5	Accepteres	n/a	5	1	5	Accepteres
11	Hack af ESDH	XXX	Tilgængelighed	2	Kan godt være nede i 1 dag	3	Serviceprovider risiko	6	Undgå	Redundans	2	2	4	Accepteres
12								0					0	
13								0					0	
14	Sagsområde 1 i ESDH	...						0					0	
15	Sagsområde 2 i ESDH	...						0					0	
16								0					0	

Ikke en eksakt videnskab

Ingen juridisk præcisering af detaljeringsgraden

Formuleret som tool:
https://virksomhedsguiden.dk/erhvervsfremme/content/ydelser/it-risikovurderingsvaerktoej/fce38da7-025d-4326-98fe-c198f3ad8316/

Kan man gøre det mere kompliceret?

Der er som nævnt ikke formkrav

- Risiko = Sandsynlighed (S) x Konsekvens (K)
- Risiko = **Fortrolighed**, S x K + **Integritet**, S x K + **Tilgængelig**, S x K
- Risiko = **Aktiv** (A-Z) (Fortrolighed, S x K + Integritet, S x K + Tilgængelig, S x K)

Anbefaling

- Operationelt
- Kan vedligeholdes
- Samme terminologi / metodik

Risikovurdering - Tool

Datatilsynet og RfDS har udgivet en lille vejledning om risikovurdering

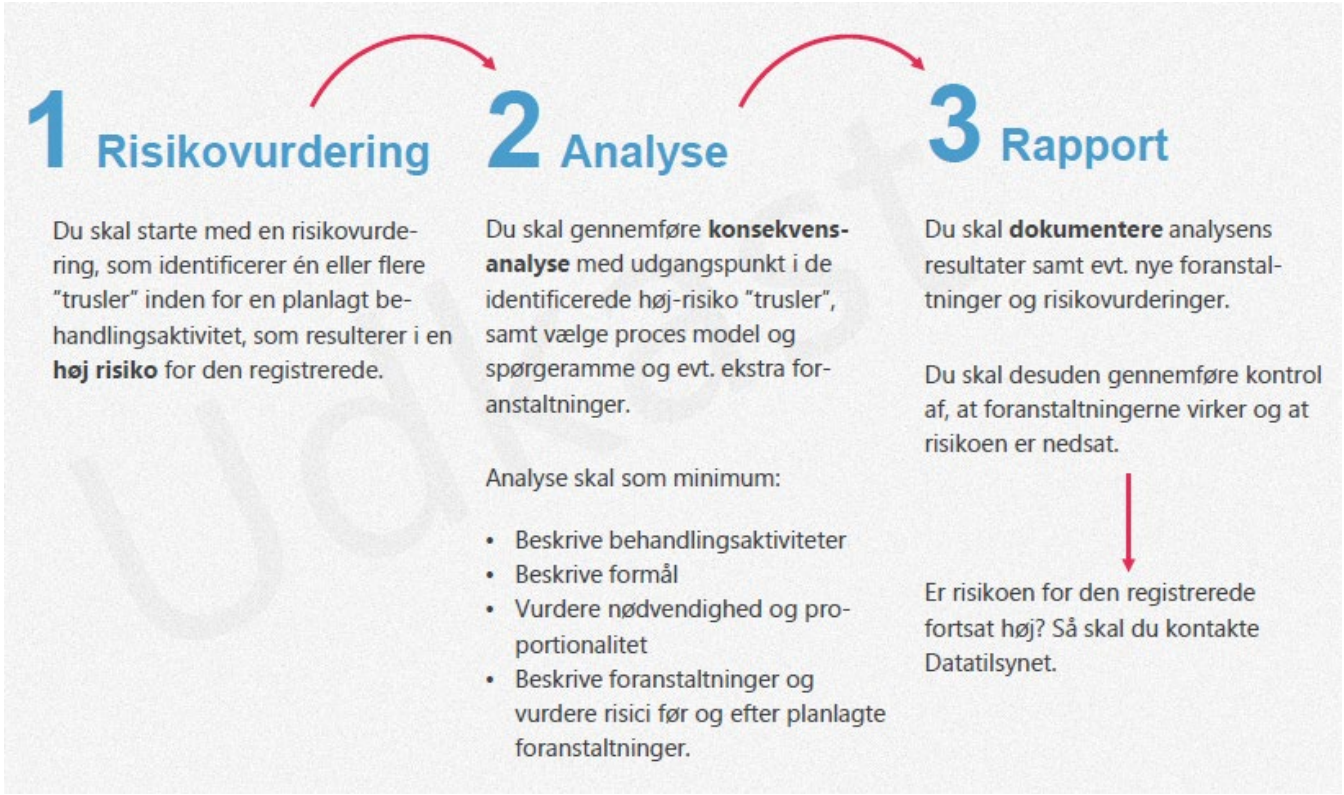
https://www.datatilsynet.dk/media/7900/vejledende-tekst-om-risikovurdering.pdf

Foranstaltninger

Husk: det er ikke gjort med risikovurderinger – der skal foranstaltninger til, som kan nedbringe risikoen

- Antivirus herunder nye typer antivirus, der også kan detektere nye vira
- Firewall
- Antispam og -phishing filtre
- IDPS (system overvågning og alarmering ved ens perimetersikring)
- Endpointsecurity
- Kryptering
- Logging
- Pseudonymisering / anonymisering
- Sårbarhedsskanning og penetrationstests
- Løbende opdatering af software, herunder vedligeholdelse af systemer ved patching
- IAM systemunderstøttelse
- Adgangskontrol baseret på multi-faktor autentifikation
- Klassifikation af data f.eks. almindelige, fortrolige, hemmelige og top-hemmelige
- Netværkssegmentering og isolering
- Mobile device management
- Backup
- Fysisk sikkerhed
- Shadow IT discovery
- Data discovery
- Data loss prevention
- Secure DNS
- Asset management
- Governance værktøj
- Styring af udstyr på netværket
- DRM
- IT-sikkerhedspolitik
- ISMS (information security manage-ment system)
- Fortegnelse over informationsaktiviteter
- Risikovurdering
- Regelsæt med mapping af GDPR og ISO27002
- Procedurer afledt af regelsæt
  - ...
  - Hændelseshåndtering
  - Beredskab
  - Intern brugerpolitik
  - Privacy notification (ekstern)
  - Data breach notification
  - Styring af leverandører
  - Kontroller
- Træning af medarbejdere og løbende awareness
- Løbende identifikation af regler og praksis
- Identity and access governance (personalesikkerhedsprocedure hos mig)

Konsekvensanalyse



Kilde: https://www.digitalsikkerhed.dk/wp-content/uploads/2021/02/RfDS-vejledning-om-konsekvensanalyse.pdf

2. Proces og spørgeramme

Spørgeramme for konsekvensanalyser

A. Beskrivelse af behandlingen/behandlingsaktiviteterne – f.eks. hvem, typer PII, omstændigheder

B. Beskrivelse af behandlingens formål – f.eks. formål, retligt grundlag, udbytte ved behandling

C. Behandlingsaktiviteternes nødvendighed og rimelighed – f.eks. mindre indgribende?, klart defineret, sagligt, rimeligt

D. Konkretisering af risici og konsekvenser – f.eks. død, begrænsning i rettigheder

E. Eksisterende og nye mulige mitigerende foranstaltninger – f.eks. cloud, AV, DLP, kontrol med databehandlere

2. Proces og spørgeramme

F.eks. A. Beskrivelse af behandlingen/behandlingsaktiviteterne

- **Hvem** behandles der oplysninger om? (kategorier af registrerede: f.eks. borgere, børn, sårbare grupper, ansatte og kunder)
- Hvilke **typer** af personoplysninger behandles der (f.eks. diagnoser, karakterer, medicin, kreditkortnummer og CPR) og hvilken følsomhed har de (f.eks. følsomme, fortrolige, straffedomme eller almindelige)
- Hvilke **omstændigheder** er der **omkring personoplysningerne**? (f.eks. antal registrerede, bredde i personoplysninger, antallet af registrerede, systematik i behandlingen (hyppighed, tidsserier) og geografisk bredde)
- Hvilke **omstændigheder** er der **om behandlingen**? (f.eks. hvorfra kommer personoplysningerne, hvordan anvendes personoplysningerne (i hvilke systemer og til hvilke beslutninger), hvordan opbevares personoplysningerne, hvem indenfor og udenfor organisationen kan tilgå data, sker der tredjelandsoverførsel og hvad er omstændighederne ved overførslen, hvor længe opbevares data (inden de slettes), anvendes der nye teknologier eller behandlingsformer, anvendes der nye teknologier eller behandlingsformer)
- Har den dataansvarlige **erfaring** med denne type behandlinger?

3. Rapport: Dokumentation, analyse

Rapport

- **Hvilke foranstaltninger**
- **Virker foranstaltningerne** / kontrol
- Er **risikoen** nedbragt?
- Hvordan **vedligeholdes** risikovurdering (udvikling i trusselsbilledet og juridisk praksis)?

PS. Lav mavefornemmelsestesten!

- **Kan jeg stå på mål for det her i byretten?**
- **Ville jeg lade mine børns oplysninger behandle på den måde?**
- **Generelt: Hvis de registreredes liv, ære og velfærd er på spil bør der laves konsekvensanalyse**

hmo@ao.dk

https://www.linkedin.com/in/henning-mortensen-343b0/

(connect gerne)