Risikovurdering
- Praktiske metoder

Rådet for Digital Sikkerhed

7. okt. 20



Henning Mortensen

Formand

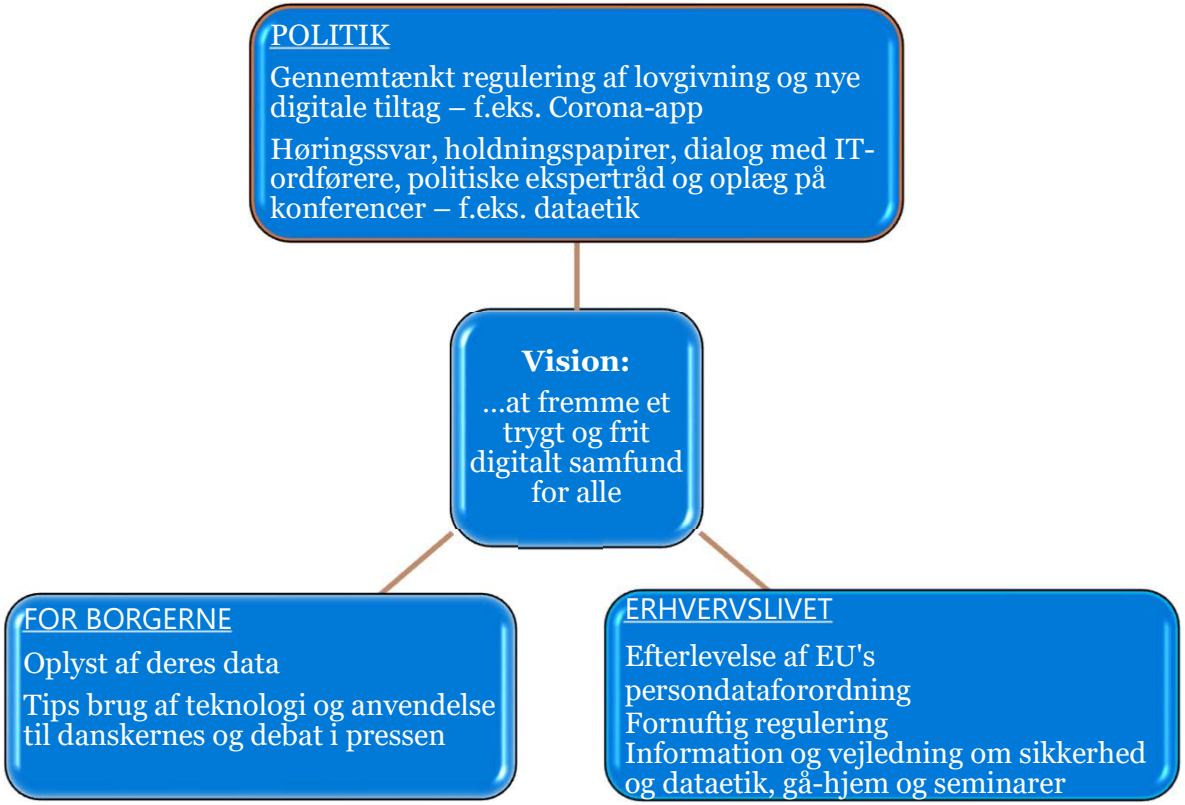
Rådet for Digital Sikkerhed

Risikovurdering i en GDPR-kontekst

– hvilke trusler står de registrerede overfor, metodikker til at samle trusselskataloger og gennemføre risikovurderinger

Om Rådet for Digital Sikkerhed

- Uafhængig medlemsorganisation indenfor informationssikkerhed og privatlivsbeskyttelse
- Ca 70 medlemmer
- Netværk, videndeling og samarbejde
- 6 Arbejdsgrupper
- Udarbejder høringssvar, holdningspapirer,
- Deltager i advisory boards for myndighederne, dialog med pressen



Disposition

- Hvad er risikovurdering?
- Trusler og trusselsterminologier
- Risikovurdering set fra organisationens versus den registreredes perspektiv
- Gennemførelse af risikovurdering
- Tools
- Foranstaltninger

Risikovurdering

Bredt koncept, der defineres forskelligt alt efter hvilket domæne det adressere, f.eks.:

- Risiko for vold
- Risiko for bortførelse
- Risiko for at få stød
- Risiko for at installation ophører med at fungere
- Risiko for økonomisk tab
- Risiko for skade

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

Aktuelle trusler - hændelser

Storytelling

- Aflytning: 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

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

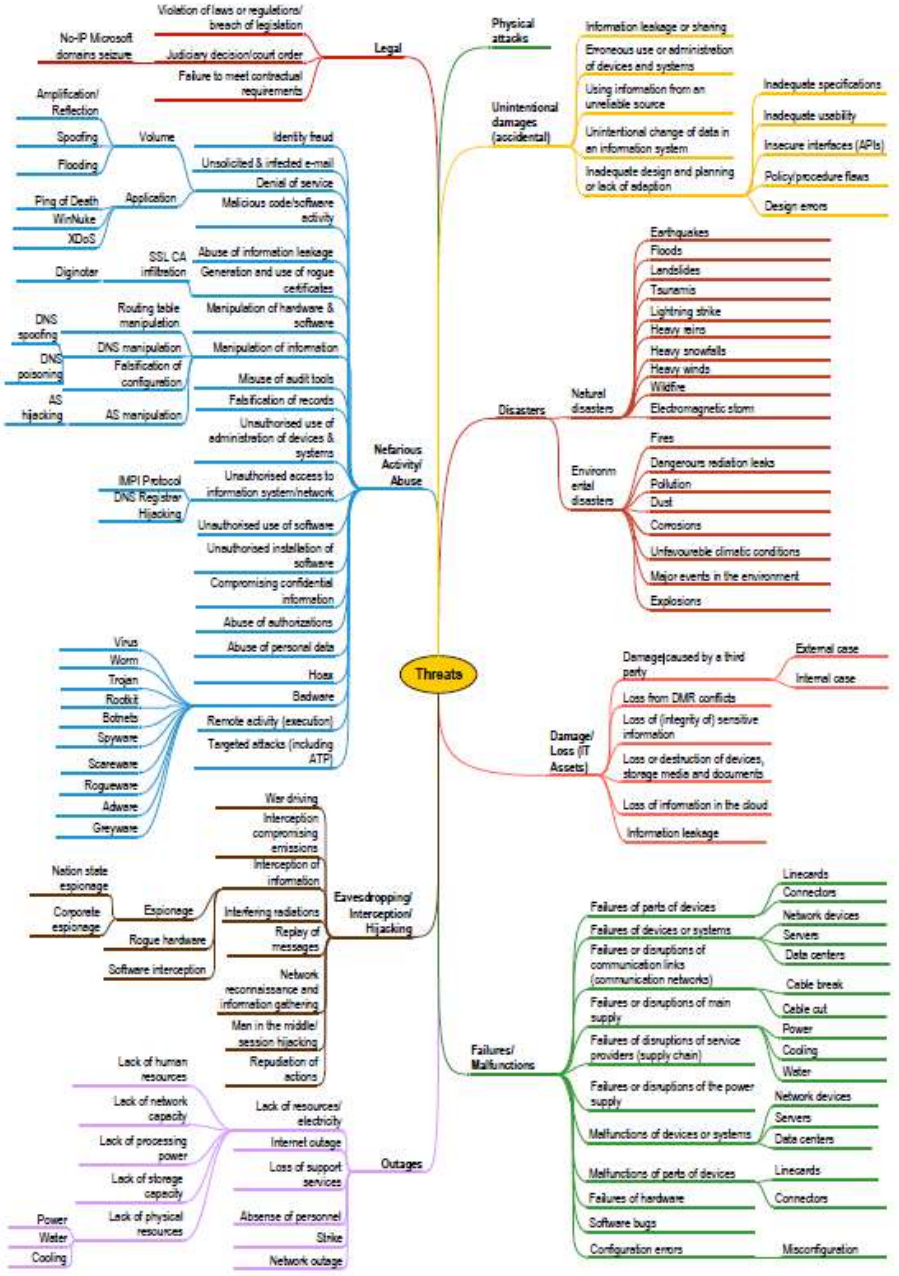
Tænk trusselsaktører

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

Trusler: ENISA

Mind map

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



Kilde:
https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

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 i informationssikkerhed

Tilgængelighed

- Ransomware
- Konsekvens: De registrerede kan ikke kontaktes; data kan ikke indgå i afgørelse

Fortrolighed

- Opsnappet personoplysninger
- Konsekvens: De registrerede eller den dataansvarlige kan afpresses; utryghed

Integritet

- Opsnappet og ændret bankkontonummer
- Konsekvens: Mister ressourcer: penge, regnekapacitet m.v.

Tre forståelser af risikovurdering

Risikovurdering

- Sandsynlighed og konsekvens
- Risiko set fra organisationens perspektiv
- 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)

Konsekvensanalyse

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

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 (nævnes 88 gange i forordningen)
- 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

Momenter af praksis

- En bemærkning om risikovurderingens "objekt":

- Fra artikel 32, stk. 1 om **Behandlingssikkerhed**: " Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende **behandling**s karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant"
- Fra præambel 75: "Risiciene for fysiske personers rettigheder og frihedsrettigheder, af varierende sandsynlighed og alvor, kan opstå som følge af behandling af personoplysninger, der kan føre til fysisk, materiel eller immateriel skade, navnlig hvis **behandlingen** kan give anledning til forskelsbehandling, identitetstyveri eller -svig, finansielle tab, skade på omdømme, tab af fortrolighed for personoplysninger…"
- Fra præampelbetragtning 76: "…Risikoen bør evalueres på grundlag af en objektiv vurdering, hvorved det fastslås, om **databehandling**saktiviteter indebærer en risiko eller en høj risiko."
- Fra præambelbetragtning 77: "…navnlig for så vidt angår identificering af risikoen i forbindelse med **behandlingen**…"

- Mange har hævdet at dette betyder, at risikovurderingens "objekt" er behandlingen

- Fra artikel 4, nr. 2: " »**behandling«: enhver aktivitet** eller række af aktiviteter — med eller uden brug af automatisk behandling — **som personoplysninger** eller en samling af personoplysninger **gøres til genstand for**, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse"

Momenter af praksis

Mere om objektet for risikovurderingen

- Selv om behandlingerne nævnes i GDPR skal man være varsom med at begrænse objektet til behandlingerne, men også risikovurdere i forhold til f.eks. trussel, data og system
- Der er ikke i GDPR nogen reference til et **bestemt framework** (i modsætning til DPIA og ISO29134 i betænkning 1565) => i skal selv vælge metodik
- Risikovurdering er **ikke en eksakt videnskab** => uanset hvad i når frem til kan det diskuteres

Faldgruber

- Hvis **objektet er behandlingsaktiviteter** – har i husket alle systemer der behandler personoplysninger?
- Hvis **objektet er systemer** – foregår der behandlinger, som ikke omfatter et (kortlagt) system (f.eks. fysiske behandlinger eller systemer, der er købt ind uden godkendelse)?

Konsekvens

- Jeg ville være **forsigtig med at stirre mig blind på behandlingen**:
  - En sårbarhed i en database, der udnyttes af en hacker til tyveri af personoplysninger, er næppe en del af de kortlagte behandlinger
  - Hvis i fokuserer snævert på jeres behandlingsaktiviteter er det ikke sikkert at i fanger alle risici
  - Det bedste er at **kombinere objekterne** efter konkret vurdering

Momenter af praksis

- Ingen steder nævnes der noget om **kvaliteten** af risikovurderingen
- I har selv domæneviden – det har jeres eksterne konsulenter og Datatilsynet ikke => der skal **meget til for at tilsidesætte jeres risikovurdering** (om end det er sket f.eks. i Intervare/Nemlig-afgørelsen, hvor DT udstedte påbud om underretning til ældre og personer med hemmelig adresse efter sikkerhedsbrud)
- Eksterne konsulenter har en tendens til at ville sælge hele metodiske frameworks => det er ikke dårligt; det kan højne både viden og modenhed og reducere risikoen for individet og organisationen, men
  - er det nødvendigt for at være compliant?
  - reagerer i på risici med foranstaltninger?
  - holder i det opdateret, når 1) i implementerer ny teknologi og 2) når der kommer nye trusler
- => jeres risikovurdering skal kunne bruges / være operationel
- Stol på jeres interne eksperter => hvis i tilsidesætter deres vurderinger, så tag ansvar for det og skriv det ned

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
- …

Summa sumarum: trusler

Kilder til trusler

- Klassiske trusselskataloger: OCTAVE, ENISA, MITRE
- Vurdering af aktuelle trusler: CFCS, DK CERT, CERT CC, sikkerhedsleverandører: McAffe, Kaspersky, Symantec, IBM,..
- Særlige privacy-orienterede trusselskataloger
- Tænk også i trusselsaktører hvem / hvad kan / vil gøre mig det ondt / handle imod mine interesser
- Jeres interne eksperter med deres faglige viden og sunde fornuft
- Netværk er vigtigt: tillid på forhånd og hurtig deling af viden

Værdien af jeres risikovurdering afhænger af at I har identificeret de rette trusler for jeres organisation

Risikovurdering

Konsekvensvurdering

- Identificer aktiver, behandlingsaktiviteter eller hvad jeres objekter for risikovurderingen er
- For hvert aktiv, hvad er så konsekvensen (stor, medium, lav) ved tab af fortrolighed, tilgængelighed og integritet

Trusselsvurdering

- Identificer trusler og fastlæg sandsynlighed (stor, medium lav)
- CfCS: "Cybertruslen mod Danmark":
  - Cyberspionage: meget høj
  - Cyberkriminalitet: meget høj
  - Cyberaktivisme: middel
  - Cyberterrorisme: lav

Sårbarhedsvurdering

- Hvilke korrigerende tiltag har vi således at vi kan reducere sandsynligheden til en given restsandsynlighed

Beskrivelse af risikobilledet

- Sammenvejning af risici, forslag til ekstra korrigerende foranstaltninger og ledelsesmæssig accept af restrisiko

ENISA breach notification

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.).

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			

Risikovurdering - Tool

Datatilsynet og RfDS har udgivet en lille vejledning om risikovurdering

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



Risikovurdering - Tool

Fra sikkerdigital.dk

https://sikkerdigital.dk/media/10255/risikovurderingsmodel.xlsx

ID	Risiko - Hvad kan påvirke fortrolighed, tilgængelighed eller integritet?	Risikoejer	Hvorfor er dette en trussel/risiko?	Skøn for Konsekvens	Hvorfor vurderes Konsekvensen til dette?	Skøn for Sansynlighed	Hvorfor vurderes sandsynligheden til dette?	Beregnet risiko	Accepteret
1	Hack af rekrutteringsystem	Hanne, HR	Sårbarhed => tabt fortrolighed	4	Individ eksponeret	4	Sket tidligere	16	Undgå
2	Intern lækage af rekruttering	Hanne, HR	Proces => tabt fortrolighed	4	Individ eksponeret	3	Leverandørs troværdighed	12	Undgå
3	Underdatabehandler kompromitteres	Hanne, HR	Proces => tabt fortrolighed	4	Individ eksponeret	3	Leverandørs troværdighed	12	Undgå
AV,	Ransomware, rekrutteringsystem	Hanne, HR	Kontrol missing => tabt	2	Individ kommer ikke i betragtning	4	Sket tidligere	8	Undgå
5	Ansøger redigerer andres data	Hanne, HR	Kontrol missing => tabt integritet	3	Individ stilles dårligere	1	Ikke kendt	3	Accepteres

Vælg mellem 1 til 5
1 Meget lille konsekvens
2 Lille konsekvens
3 Nogen konsekvens
4 Høj konsekvens
5 Meget stor konsekvens

Vælg mellem 1 til 5
1 Sjælden eller usandsynlig
2 Vil næppe forekomme
3 Er mulig
4 Må forventes at kunne ske
5 Vil blive udnyttet

Risikohåndtering

Nye foranstaltninger	Konsekvens efter nye foranstaltninger	Ny sansynlighed	Ny restrisiko	Restrisiko Accepteret	Konklusion	Risikovillighed	Forklaring
Sårbarhedsskanning	4	2	8	Forsikring	Kan ikke nedbringes mere	Grøn	
Procedure, SIEM, DLP	4	1	4	Accepteres		1	Ledelsens vurdering af laveste risikoscore som er GRØN
Audit	4	2	8	Forsikring	Kan ikke nedbringes mere	Gul	
AV, Pakkeanalyse	2	2	4	Accepteres		6	Ledelsens vurdering af laveste risikoscore som er GUL
n/a			0			Rød	
			0			10	Ledelsens vurdering af laveste risikoscore som er RØD

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)

Målet!

Beskytte de registreredes **fundamentale rettigheder** mod vores behandlinger

Vores **foranstaltninger** i form af teknologi, politikker og procedurer **er bare midler til at nå målet**

Vi skal altså **reducere risikoen** for at de registreredes fundamentale rettigheder krænkes

Kontakt

Henning Mortensen

hmo@ao.dk