Informationssäkerhet – en praktisk överblick

Agne Lindberg, den 30 maj 2024

BG Institute
EN DEL AV BLENDOW GROUP

IT- och informationssäkerhet i juridiken

- Regulatoriska krav (Fokus på GDPR och Cybersäkerhetslagen)
- Leverantörskedjan: IT-leveransavtalet en viktig komponent
- Verksamhetsstyrning
- Tillsyn och sanktioner

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Den rättsliga kartan

Skydd av enskilda

- GDPR
- Patientsäkerhet

Skydd av viktig infrastruktur

- NIS (Lag om informationssäkerhet i samhällsviktiga och digitala tjänster), Cybersäkerhetslagen
- CER direktivet (motståndskraft)

Skydd för förtroende, underlätta för kunder/konsumenter

- Cyberresiliance Act, Cybersäkerhetsförordningen

Ansvar

- Vem ansvarar? GDPR, AI-förordningen
- Även avtalsfrågor

CER-direktivet

- Bredare än cybersäkerhet – även andra hot (terror, sabotage, naturkatastrof)
- Nationell strategi, nationell riskbedömning
- Identifiera risker – lämpliga tekniska, organisatoriska och säkerhetsmässiga åtgärder. Incidentrapportering.
- Förslag i september 2024

MSB

- Förordning om myndigheters beredskap (inkl IT incident rapportering)
- Föreskrifter från MSB: 2020:6 infosäkerhet + 2020:7 om säkerhetsåtgärder + 2020:8 om incidentrapportering

SOU 2024:18 – Cybersäkerhetslagen

- Från och med 1 januari 2025 – implementerar NIS 2-direktivet i Sverige

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

...varför är det relevant?

47 000 elevers personuppgifter läckta – ligger ute till försäljning

Göteborg • Nästan alla Göteborgs grundskoleelevers personuppgifter har laddats ner av en okänd person. Det handlar om 47 000 elever, vars uppgifter nu ligger ute på en sajt och erbjuds till försäljning.

23 JAN 2018 SAMHÄLLE

80 personer kom åt hemlig svensk information – rör skydd mot terrorism

Ett 80-tal personer utan svensk säkerhetsklassning har haft tillgång till Transportstyrelsens it-system i drygt två år.

Cyberattack mot vindkraftskoncern – stängt av sina it-system

I torsdags upptäckte tyska Nordex Group att man utsattes för en hackerattack. Attacken tvingade vindkraftskoncernen att stänga av sina it-system.

23 augusti, 2017

Maersk förlorade över 200 miljoner dollar till följd av cyberattack

Tidigare i sommar drabbades den danska rederikoncernen Maersk

Cyberattacker mot Valmyndigheten

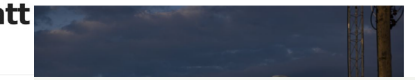
Valmyndigheten har haft stora teknikproblem under valkvällen. Bland annat har myndigheten utsatts för flera överbelastningsattacker.

Dokument bekräftar: Synsam blev hackat av utpressare

PUBLICERAD 2020-10-14

Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad



Nyheter

Finlands riksdag utsatt för cyberattack

Av: TT

PUBLICERAD: 9 AUGUSTI

SVERIGE

Känsliga uppgifter i fara efter cyberattack mot Transportstyrelsen

UPPDATERAD 2022-06-05 PUBLICERAD 2022-06-05

SVERIGE

Data stals vid cyberattacken mot Naturvårdsverket

UPPDATERAD 2022-10-06 PUBLICERAD 2022-10-06

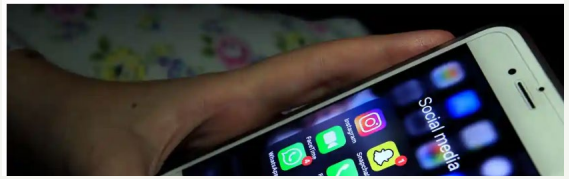
Tusentals journaler läckta från finskt terapiföretag

UPPDATERAD 28 OKTOBER 2020 PUBLICERAD 27 OKTOBER 2020

Tusentals patientjournaler från finska vårdbolaget Vastaamo har läckt i vad som beskrivs som en omfattande och sällsynt hackerattack. Patienter vars journaler läckt har utpressats att betala pengar för att stoppa spridningen av de privata uppgifterna på nätet.

Instagram owner Meta fined €405m over handling of teens' data

Penalty follows investigation into Instagram setting that allowed teenagers to set up accounts that displayed contact details



Montenegro hårt drabbat av cyberattack – pågått i tre veckor

En samordnad cyberattack mot statsapparaten i Montenegro har pågått sedan 20 augusti. Attacken misstänks komma från Ryssland.

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Informationsklassning nödvändig

- Informationssäkerhet – riskbaserade åtgärder. Behov av olika nivåer för olika typer av information
- Exempel
  - Personuppgifter (vanliga, känsliga, brott, personnummer).
  - Risknivåer – styr krav på säkerhetsåtgärder, access, kontroller
    - Publik – Intern – Konfidentiell
  - Del av informationssäkerhetspolicy/riktlinjer
  - Styr även leverantörsavtalet

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Regulatoriska krav

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

GDPR – några relevanta krav

- PuA:
  - Privacy by design (Art 25) – tekniska och organisatoriska åtgärder för att uppfylla kraven i GDPR och skydda enskilds rättigheter/endast behandling
    - EDPB riktlinjer 4/2019
  - Utkontraktering – avtalskrav (Art 28). Exempel: Krav på sekretessåtagande, åtgärder enl Art 32, underbiträden, bistå PuA i fullgörande av Art 32-36

- PuA och PuB: Lämplig säkerhetsnivå – tekniska och organisatoriska åtgärder lämpliga i förhållande till **risken** (Art 32), inbegripet (”när det är lämpligt”):
  - Pseudonymisering och kryptering
  - Konfidentialitet, integritet och tillgänglighet hos systemen
  - Regelbundna tester
  - Inga konkreta krav!
  - Motivera och dokumentera (notera Artikel 5.2): ”Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (*ansvarsskyldighet*).

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Cybersäkerhetslagen

- Ersätter lag om informationssäkerhet för samhällsviktiga och digitala tjänster fr. o. m. 1 januari 2025
- Viktiga nyheter:
  - Nationella åtaganden och samarbete inom EU. Krav på cyberkrishanteringsmyndighet och CSIRT team
  - Fler sektorer
  - Omfattar hela verksamheten – inte bara den verksamhet som leder till tillämplighet
  - Tydligare krav på Leverantörskedjan
  - Högre sanktioner/nya sanktioner
- Regler om riskhanteringsåtgärder eller incidentrapportering med ”motsvarande verkan” tar över cybersäkerhetslagen.
  - DORA
  - GDPR?

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Vilka omfattas?

- Energi (elektricitet, fjärrvärme/-kyla, olja, gas och vätgas)
- Transporter (lufttransport, järnvägstransport, sjöfart och vägtransport)
- Bankverksamhet
- Finansmarknadsinfrastruktur
- Hälso- och sjukvård
- Dricksvatten
- Avloppsvatten
- Offentlig förvaltning (myndigheter, kommuner, regioner) *Undantag: Regeringen, myndigheter under Riksdagen och domstolar + 16 myndigheter med känslig verksamhet*
- Post och budtjänster

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Vilka omfattas? forts.

- Avfallshantering
- Tillverkning, produktion och distribution av kemikalier
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning (bl. a. datorer, medicintekniska produkter, motorfordon)
- Digitala infrastruktur (molntjänster, datacentraltjänster, leverans av innehåll m.m.)
- Digitala leverantörer (marknadsplatser, sökmotorer, sociala nätverk)
- IKT-tjänster (hanterade tjänster – säkerhetstjänster) – mellan företag
- Forskning
- Rymden
  - Generellt storlekskrav för att omfattas: Minst 50 personer eller årsomsättning som överstiger 10 MEUR
  - Uppdelning i väsentliga och viktiga verksamhetsutövare

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Krav på verksamhetsutövare – riskhanteringsåtgärder (3 kap.)

- OBS – hela verksamheten omfattas, inte bara den verksamhet som ”triggar” lagens tillämplighet
- Anmälan till tillsynsmyndighet: identitet, kontaktuppgifter, verksamhet
- Riskhanteringsåtgärder
  - Riskanalys – riskexponering, sannolikhet och konsekvenser
  - Proportionella åtgärder baserat på riskanalys
  - Dokumentera!
- Konkret om riskhanteringsåtgärder:
  - Ska hantera och identifiera risker i nätverks- och informationssystem + systemens fysiska miljö
  - Syfta till att förhindra incidenter eller minimera påverkan
  - Viktiga aspekter: *tillgänglighet, autenticitet, riktighet och konfidentialitet*
  - Obligatoriska moment! (se nästa sida)

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Riskhantering – obligatoriska moment

- *Incidenthantering*,
- Kontinuitetshantering (backup, BCP, DR). Behov av att bedöma RPO (hur färsk data) & RTO (tid för återläsning)
- *säkerhet i leveranskedjan,*
- säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem inklusive hantering av sårbarheter och sårbarhetsinformation, Avser köp! Inte exempelvis utkontrakteringn (träffas av säkerhet i leveranskedjan)
- strategier och förfaranden för användning av kryptografi och kryptering,
- personalsäkerhet,
- strategier för åtkomstkontroll och tillgångsförvaltning,
- säkrade lösningar för kommunikation, och
- lösningar för autentisering.
- Föreskrifter kommer! Behov av informationsklassning! Baserat på lagkrav, värde, hot och kostnad. Komplettera med spårbarhet!

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Riskhantering – systematiskt informationssäkerhetsarbete

- Verksamhetsutövare ska bedriva systematiskt och riskbaserat informationssäkerhetsarbete. Föreskrifter kommer!
- Viktiga moment:
  - Långsiktigt – Kontinuerligt - Metodiskt
  - Rollfördelning med särskilt utpekat ansvar
  - Kontroll/tester/uppdatering
  - Ska göra att ledningen kan styra arbetet och utvärdera (jfr Art 20.1 – ledningsorgan (styrelsen) ska godkänna och övervaka riskhanteringsåtgärder – Se även ABL 8 kap 4§). ’’
  - ISO 27001 – inte uttryckligt krav, men innehåller de nödvändiga momenten (etablera, implementera, driftsätta, övervaka och underhålla/förbättra informationssäkerhet (ISMS).
- Även utbildning är viktig!
  - Ledningen obligatoriskt (Styrelse resp. GD + stab + kommun- och regionstyrelse).
    Övriga anställda - erbjudas

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Krav på verksamhetsutövare - incidentrapportering

- Incident: *en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom nätverks- och informationssystem*
- Vilka incidenter?
  - Cybersäkerhetslagen: Betydande incident - Orsakat eller KAN orsaka allvarliga driftstörningar för tjänsten eller ekonomisk skada för verksamhetsutövaren ELLER som kan påverka andra genom betydande materiell eller immateriell skada.
  - GDPR: Säkerhetsincident som leder till förstöring, förlust, ändring eller obehörigt röjande/åtkomst av personuppgifter
- När:
  - Cybersäkerhetslagen: Varning till MSB inom 24 timmar från kännedom. Incidentanmälan inom 72 timmar (betrodda tjänster: 24 timmar). Slutrapport inom en månad.
  - GDPR: Inom 72 timmar från kännedom.
  - MSB: Inom 6 timmar. Slutrapport inom 4 veckor.
- Innehåll:
  - Cybersäkerhetslagen: Anmälan - Incidentens art och hur allvarlig. Konsekvenser. Angreppsindikatorer. Slutrapport: Detaljerat innehåll inkl. åtgärder
  - GDPR: Innehåller inte krav på allvarlighetsgrad och angreppsindikatorer – endast art, sannolika konsekvenser, åtgärder, kontaktuppgifter samt kategorier och antal av personuppgifter

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Krav på verksamhetsutövare – incidentrapportering, forts.

- Information:
  - Cybersäkerhetslagen: Alla kunder som kan antas påverkas. Gäller även för cyberhot.
  - GDPR: ”sannolikt att leder till hög risk för fysiska personers rättigheter och friheter”.

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Krav på verksamhetsutövare – Leverantörskedjan

- Riskhanteringsåtgärder behöver speglas mot leverantörer
- *SKÄL 85: ... särskilt viktigt att hantera risker som härrör från en entitets leveranskedja och dess förhållande till sina leverantörer, såsom leverantörer av datalagrings- och databehandlingstjänster eller leverantörer av hanterade säkerhetstjänster …, med tanke på förekomsten av incidenter där entiteter har varit föremål för cyberattacker och där inkräktare med avsikt att vålla skada har kunnat äventyra säkerheten i en entitets nätverks- och informationssystem genom att utnyttja sårbarheter som påverkar tredje parts produkter och tjänster. … entiteter bör därför bedöma och beakta den övergripande kvaliteten och resiliensen hos produkter och tjänster och de riskhanteringsåtgärder för cybersäkerhet som är inbyggda i dem samt cybersäkerhetspraxis hos sina leverantörer och tjänsteleverantörer, inbegripet deras förfaranden för säker utveckling. Väsentliga och viktiga entiteter bör framför allt uppmuntras att införliva riskhanteringsåtgärder för cybersäkerhet i avtal med sina direkta leverantörer och tjänsteleverantörer.*

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Leverantörskedjan – en checklista – val av leverantör / riskbedömning

- Planering av säkerhet kräver att organisationen identifierar risker – inkl leverantörer
- Leverantörskedjan
  - Riskbedömning (access till vilken data, underleverantörer, säkerhetsåtgärder etc)
- Process för att utvärdera och välja leverantör
  - Upphandlingskrav
  - Referenser
- Krav på avtalets innehåll

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Avtalet – en checklista

- Inkludera lämpliga säkerhetsåtgärder i leverantörsavtal
  - Tydliga krav på relevanta delar av de obligatoriska punkterna. Särskilt viktigt:
    - Business Continuity / Disaster Recovery
  - Servicenivåer – mätbara krav
    - Backup/RTO/RPO
    - Resolution time
    - Implementering av tredjeparts patchar
    - Antal återställandetester
  - Krav på leverantörens kontroll: Revisioner, rapportering, tester
  - Underleverantörer – kontroll, spegla krav

- OBS – branschsspecifika krav – EBA, Dora

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Verksamhetsstyrning

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Styrning / ledningssystem - Styrdokument som behövs - checklista

- Fastställs av ledningen. Kommuniceras.
- Policy
  - Grundläggande principer och värderingar
    - IT-policy
    - Informationssäkerhetspolicy
- Riktlinjer - Förtydligar och konkretiserar
  - Informationsklassning
  - Access/behörighet
  - Change
  - Personuppgiftshantering
  - Övervakning, incident och problem
  - BCP / Disaster Recovery
  - Visselblåsning
- Innehåll
    - Vem beslutar? Vem ”äger”? Roller och ansvar!
    - Uppdateringsansvar
    - Kontroll och uppföljning

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Tillsyn och sanktioner

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Tillsynsmyndigheter

NIS1

Tabell 3.1 Tillsyn

Sektor	Tillsynsmyndighet
Energi	Statens energimyndighet
Transporter	Transportstyrelsen
Bankverksamhet	Finansinspektionen
Finansmarknadsinfrastruktur	Finansinspektionen
Hälso- och sjukvård	Inspektionen för vård och omsorg
Leverans och distribution av dricksvatten	Livsmedelsverket
Digital infrastruktur	Post- och telestyrelsen
Digitala tjänster	Post- och telestyrelsen

Cybersäkerhetslagen

- Statens energimyndighet för energisektorn
- Transportstyrelsen för transportsektorn och delar av tillverkningssektorn Finansinspektionen för bank- och finansmarknadsinfrastruktursektorerna
- Inspektionen för vård och omsorg (IVO) för delar av hälso- och sjukvårdssektorn
- Läkemedelsverket för en del av hälso- och sjukvårdssektorn och en del av tillverkningssektorn
- Livsmedelsverket för sektorerna dricksvatten, avloppsvatten samt produktion, bearbetning och distribution av livsmedel
- Post- och telestyrelsen för sektorerna digital infrastruktur, digitala leverantörer, förvaltning av IKT-tjänster, post- och budtjänster samt rymdsektorn
- Länsstyrelserna i Stockholms, Skåne, Västra Götalands och Norrbottens län för sektorerna offentlig förvaltning, avfallshantering, forskning, en del av tillverkningssektorn och tillverkning, produktion och distribution av kemikalier samt lärosäten med examenstillstånd.

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Tillsynsmyndigheten

- Undersökningsbefogenheter
  - Differentiering mellan väsentliga och viktiga verksamhetsutövare
  - Begära information och tillgång till lokaler
    - Förenas med föreläggande och eventuellt vite. Handräckningsmöjlighet.
  - Ålägga att utföra riktade säkerhetsrevisioner av oberoende organ
    - Tillsynsmyndighet får anlita oberoende organ för regelbundna revisioner av *väsentliga* verksamhetsutövare.
  - Genomföra säkerhetsskanningar. Inte penetrationstest!
  - Får meddela föreskrifter om riskhanteringsåtgärder + systematiskt arbete + utbildning

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Sanktioner

- Ingripande ska ske vid vissa brott mot cybersäkerhetslagen, exempelvis:
  - Anmälningsskyldighet
  - Riskhanteringsåtgärder 3 kap. 1 § (”obligatoriska listan”)
  - Utbildning enligt 3 kap. 3 §
  - Incidentrapportering (rapportering 24h/72h/1 månad – 3 kap. 5-7 §§)
- Ingripanden:
  - Föreläggande – kan förenas med vite
  - Förbud att utöva ledningsfunktion (förvaltningsdomstol) – allvarlig överträdelse av uppsåt/grov oaktsamhet
  - Sanktionsavgift
    - Väsentliga: Högsta av 2% av global årsomsättning/10 MEUR
    - Viktiga: Högsta av 1,4% av global årsomsättning/7 MEUR
    - Offentlig verksamhet: Max 10 MSEK
  - Alternativt: Anmärkning - varning

Delphi

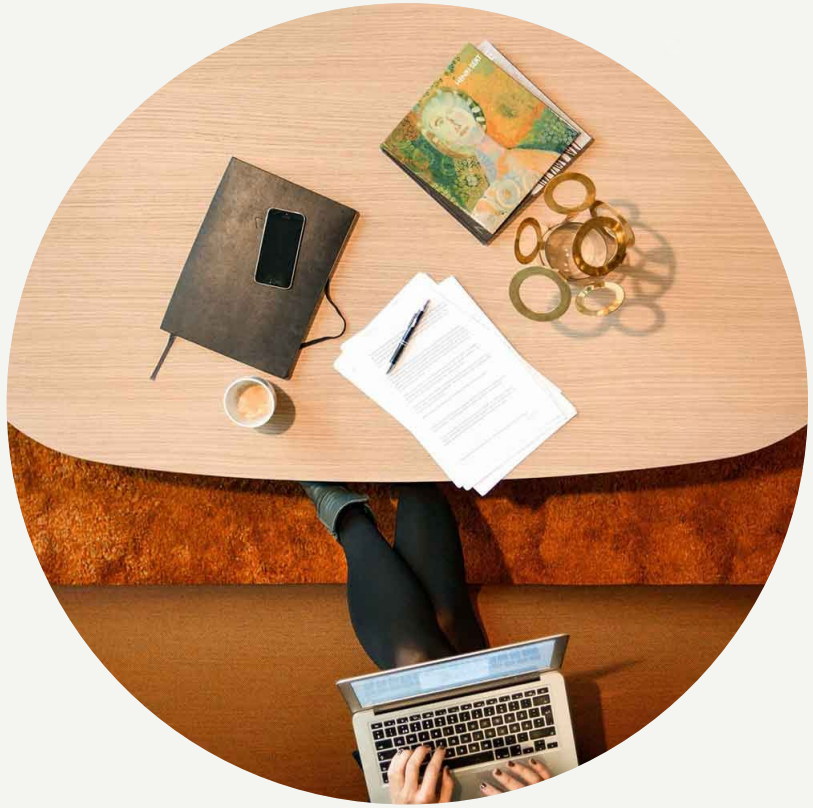
BG Institute
EN DEL AV BLENDOW GROUP

Informationssäkerhet - checklista

- **Kontroll över informationsflöden**
  - Kategorisering av data – styr tillämpliga regler (t.ex. personuppgifter) och säkerhet
  - Informationsklassning hjälper oss att prioritera säkerhetsarbetet
- **Lämpliga riskhanteringsåtgärder**
  - Parallella regler ställer olika krav – lägg skyddet på högsta tillämpliga nivå
  - Systematik fångar upp nya/förändrade risker och säkerhetskrav

  Dokumentera och följ upp
  - Dokumentera vad som görs, hur incidenter hanteras och ägarskap. Testa rutiner med periodicitet
  - Top-Down - styra och kontrollera

  Avtalet
  - Leverantörskedjan viktigt. Analysera både leverantör och avtal. Avtalet ska återspegla tekniska och organisatoriska åtgärder. Servicenivåer? Revisionsrätt
  - Ställ krav på leverantörer och verifiera löpande



Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Informationssäkerhet – juridiken och det praktiska arbetet med compliance

25 september kl. 09.00 – 16.00 med Agne Lindberg

Denna heldagskurs följer upp och fördjupar dagens webbinarium. Som deltagare får du kunskap om:

- Information om den rättsliga kartan – bl.a. NIS 2, GDPR och AI-förordningen
- Hur hanteras informationssäkerhet i IT-avtal
- Praktiska råd för hur man tar fram och implementerar policies för IT och informationssäkerhet
- Hur man arbetar praktiskt med informationssäkerhet

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Vad tyckte du om dagens webbinarium?

Ta gärna 30 sekunder och svara på frågorna I fliken “Polls” under chattfliken.

Tack för dina synpunkter!

Delphi

BG Institute
EN DEL AV BLENDOW GROUP

Frågor?

Delphi

BG Institute
EN DEL AV BLENDOW GROUP