GDPR och cybersäkerhet

6 december 2018

Mats Kellqvist

pwc

Status ett halvår efter att lagen har trätt i kraft

Om Datainspektionens granskningar

- Myndigheten har hittills koncentrerat sig på legala processer, vilket i och för sig inte är konstigt då Datainspektionens 80 medarbetare i huvudsak är jurister och Datainspektionens roll som tillsynsmyndighet.

- Datainspektionen har undersökt om 400 myndigheter och offentliga företag har tillsatt en DSO. Varningar har utfärdats men inga böter.

- Ytterligare utredningar kring samtyckeshantering, personuppgiftsansvariga och personuppgiftsbiträden.

- Datainspektionen ska även utreda om ett antal myndigheter efterlever brottsdatalagen och kraven om att behålla skriftliga uppgifter.

- Även undersöka organisationers agerande kring frågor från de registrerade, såsom registerutdrag, radering och portering.

Datainspektionens första GDPR-granskningar

Publicerad 2018-10-23

Första svenska GDPR-granskningen klar

Datainspektionen har undersökt om drygt 400 företag och myndigheter har utsett ett dataskyddsombud. Granskningen visar bland annat brister hos närmare en fjärdedel av de fackförbund som valts ut för kontroll.

Enligt dataskyddsförordningen, GDPR, är alla myndigheter och även vissa företag skyldiga att utse ett dataskyddsombud. Ombudet ska kontrollera att den egna organisationen följer bestämmelser och interna styrdokument om dataskyddsfrågor och informera och ge råd internt.

- Det är en väldigt viktig roll för att öka medvetenheten och regelefterlevnaden av GDPR, vilket är skälet till att vi prioriterat detta som vår första GDPR-granskning, säger Datainspektionens generaldirektör Lena Lindgren Schelin.

Datainspektionen har gjort en bred granskning av drygt 400 myndigheter och företag och undersökt om de utsett ett dataskyddsombud och om de dessutom meddelat detta till Datainspektionen, vilket de måste göra.

Granskningen visar att majoriteten av de granskade organisationerna har anmält och utsett ett dataskyddsombud i tid. Vissa branscher utmärker sig dock negativt. Av de 51 fackförbund som fanns med i urvalet hade närmare 25 procent brister.

- Eftersom det gått så pass kort tid efter att GDPR infördes den 25 maj, har vi stannat vid att utfärda reprimander. Men, skulle vi framöver konstatera fortsatta brister när det gäller dataskyddsombud så kan även administrativa sanktionsavgifter bli aktuella, säger Lena Lindgren Schelin.

Publicerad 2018-10-19

Datainspektionen inleder fler granskningar

Datainspektionen drar nu igång flera större granskningar av olika delar av dataskyddsförordningen, bland annat vad gäller samtycke som rättslig grund för att samla in och behandla personuppgifter.

Datainspektionen drar under hösten igång flera större granskningar. Syftet med granskningarna är bland annat att skapa vägledning gällande de nya dataskyddsreglerna i bland annat dataskyddsförordningen, GDPR. Ett av projekten fokuserar på samtycke som rättslig grund för att samla in och använda personuppgifter.

- Samtycke är speciellt eftersom det måste lämnas frivilligt och det inte får finnas för stor ojämlikhet mellan den registrerade personen och den personuppgiftsansvarige, säger Datainspektionens generaldirektör Lena Lindgren Schelin.

- Samtycken ska också kunna återkallas, vilket ställer stora krav på verksamhetsutövarna att ha strukturer och rutiner för detta. Vi har sett att samtycken ibland samlas in trots att behandlingen kan motiveras på annan grund. Här behövs vägledning, säger hon.

Ett annat projekt ska klargöra gränsdragningen mellan personuppgiftsansvarig och personuppgiftsbiträde.

- Många av dagens it-lösningar bygger på att ett biträde sköter driften åt den som är ansvarig för de personuppgifter som hanteras. Det finns flera frågor som rör gränsdragningen mellan dessa roller som är viktiga att utreda.

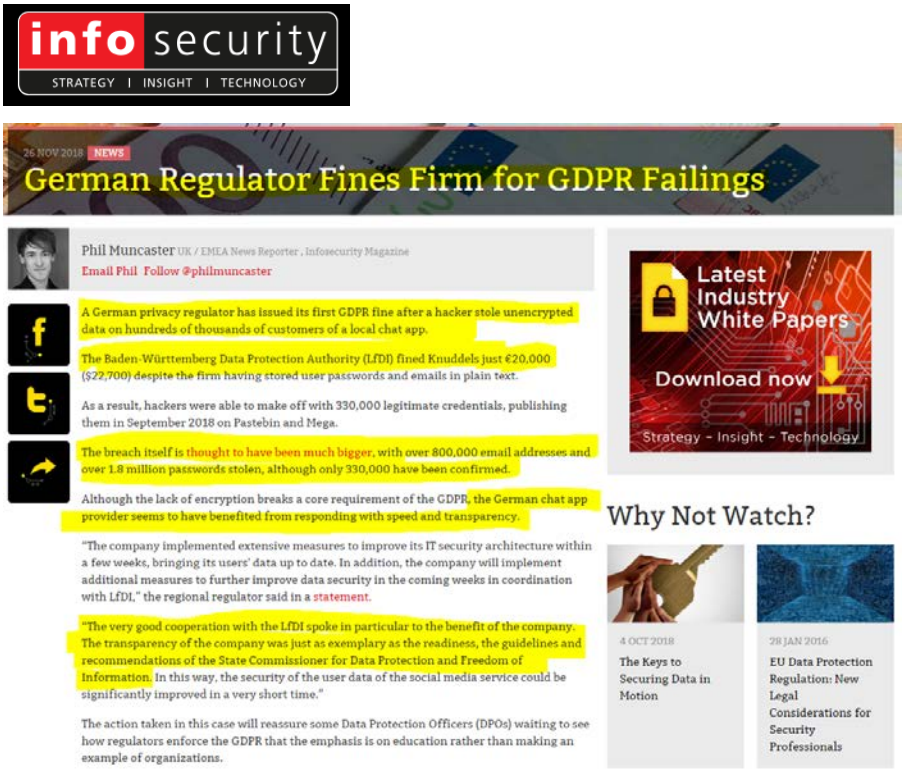
I ett tredje tillsynsprojekt fortsätter den granskning av dataskyddsombud som inleddes i juni. Efter den granskningen fann Datainspektionen anledning att även titta på den information som ska ges till de registrerade om vem som är dataskyddsombud och hur denne kan kontaktas.

- Det här är de stora, planerade granskningar som vi genomför under hösten. Till detta kommer även ytterligare granskningar som vi kan komma att inleda efter till exempel klagomål eller på eget initiativ när det finns brister som bedöms vara så pass allvarliga att de behöver granskas närmare, säger Lena Lindgren Schelin.

Den första GDPR-sanktionen i Tyskland

Baden-Würtenbergs datainspektion blev först ut att bötfälla för GDPR-brott.

Sanktionen blev ovanligt mild, men kan dels beror på att det var den första sanktionen och att dels företaget var exemplariskt med att samarbeta och lösa problemet på ett professionellt sätt.



info security
STRATEGY | INSIGHT | TECHNOLOGY

26 NOV 2018 NEWS

German Regulator Fines Firm for GDPR Failings

Phil Muncaster UK / EMEA News Reporter, Infosecurity Magazine
Email Phil Follow @philmuncaster

A German privacy regulator has issued its first GDPR fine after a hacker stole unencrypted data on hundreds of thousands of customers of a local chat app.

The Baden-Württemberg Data Protection Authority (LfDI) fined Knuddels just €20,000 ($22,700) despite the firm having stored user passwords and emails in plain text.

As a result, hackers were able to make off with 330,000 legitimate credentials, publishing them in September 2018 on Pastebin and Mega.

The breach itself is thought to have been much bigger, with over 800,000 email addresses and over 1.8 million passwords stolen, although only 330,000 have been confirmed.

Although the lack of encryption breaks a core requirement of the GDPR, the German chat app provider seems to have benefited from responding with speed and transparency.

"The company implemented extensive measures to improve its IT security architecture within a few weeks, bringing its users' data up to date. In addition, the company will implement additional measures to further improve data security in the coming weeks in coordination with LfDI," the regional regulator said in a statement.

"The very good cooperation with the LfDI spoke in particular to the benefit of the company. The transparency of the company was just as exemplary as the readiness, the guidelines and recommendations of the State Commissioner for Data Protection and Freedom of Information. In this way, the security of the user data of the social media service could be significantly improved in a very short time."

The action taken in this case will reassure some Data Protection Officers (DPOs) waiting to see how regulators enforce the GDPR that the emphasis is on education rather than making an example of organizations.

Vanliga missförstånd om GDPR

- Alla måste ha ett dataskyddsombud
- Anlita ett personuppgiftsbiträde = avskriva sig ansvar
- Samtycke och kryptering ett måste
- Efter 25 maj kan man lägga GDPR arbetet lite åt sidan
- Nyheter i GDPR går före grundläggande krav i PuL

PwC:s granskningar

PwC har hjälpt 120 företag att forma GDPR-lösningar.

Vi har hunnit göra formella granskningar av cirka 25 organisationer.

Iakttagelser (processmässiga):

- Ju större organisation, desto större och fler brister. Många gånger frapperande, elementära brister, som till exempel att register saknas på vilka personuppgifter som finns.
- Organisationerna överskattar nästan alltid sitt eget arbete. De anser att processer och lösningar är klara, när verkligheten säger något helt annat.
- Företagsledningen har inte avdelat resurser (tid och pengar) för att arbeta med frågan. Avdelningarna har heller inte äskat resurser.
- Alltför ofta har GDPR-arbetet gjorts som en juridisk övning, frånkopplad it- och informationssäkerheten.
- Alternativt har man arbetat med informationssäkerheten och ignorerat den legala aspekten.
- Vissa tycks resonera att nu har den 25 maj passerats och att nu behöver man inte längre arbeta med GDPR (anmärkningsvis ofta de som knappt alls har tagit i frågan).

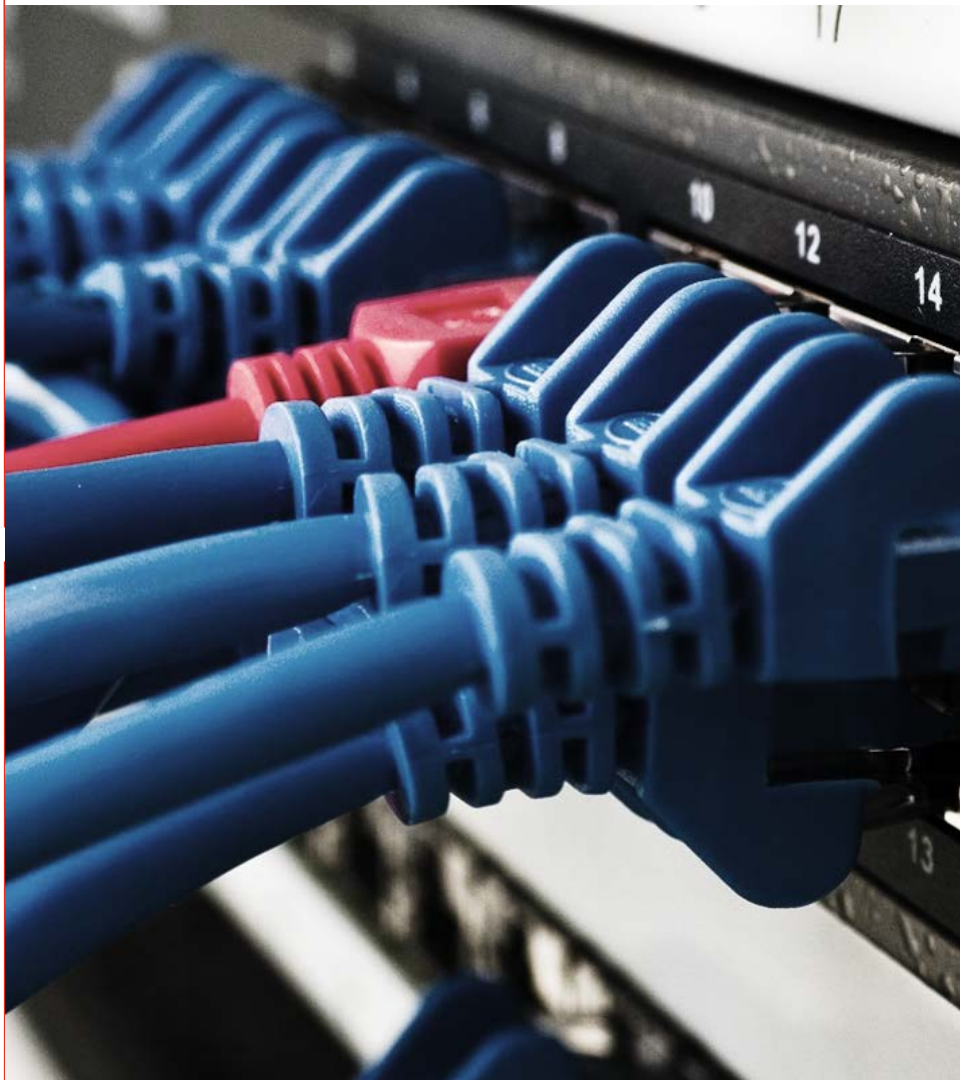
PwC:s granskningar (forts)

Iakttagelser (it-säkerhet):

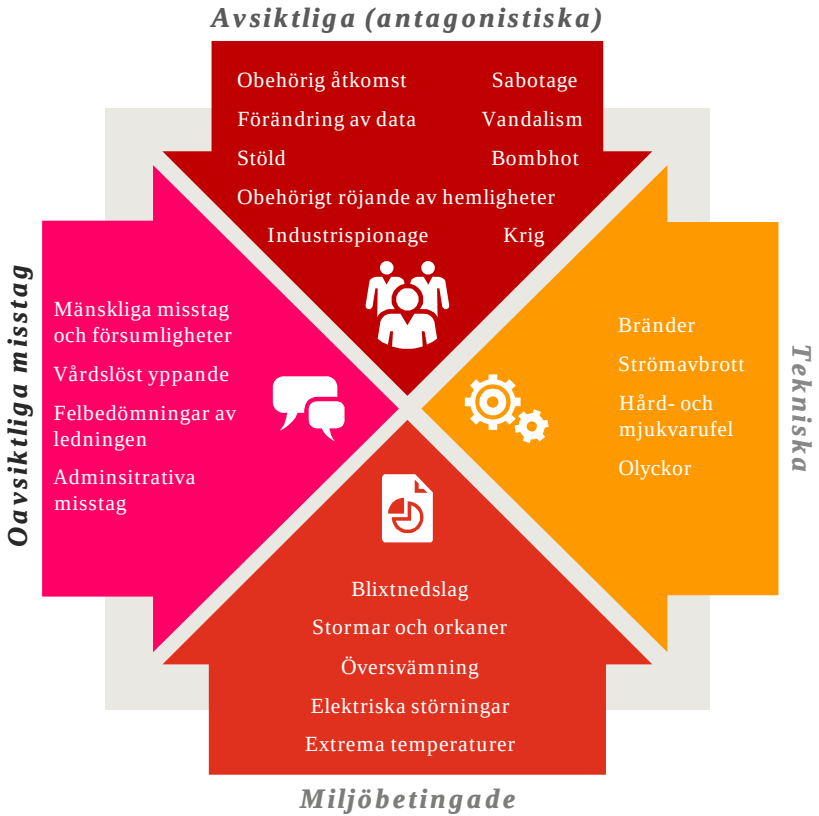
(Dessa granskningar har inte beställts för att granska GDPR, men utav andra anledningar. Vi vet dock att dessa system innehåller känsliga personuppgifter och kan dra dessa slutsatser om personuppgifterna)

- *Behörighetshantering* är den mest påtagliga bristen i de interna systemen. Alltför många ges behörighet till alltför många system och kan ”nästla” sig vidare och därmed skulle de kunna läsa och ändra andras känsliga information.
- Webblösningar som kundportaler har satts upp felaktigt utan *autentiseringsskydd*, för svag *behörighetskontroll* och undermålig *lösenordshantering*. Möjlighet finns att utifrån komma åt känsliga data.
- *Incidenthanteringsprocesser* saknas för att utreda och förbättra säkerheten baserat på inträffade händelser. Tekniska förutsättningar saknas att utreda.
- I allmänhet är det tekniska skyddet av företagens och myndigheters information mycket svagt, vilket även gäller personuppgiftsinformation.

Cybersäkerhetshot



Hotbilder


Avsiktliga (antagonistiska)
Obehörig åtkomst
Sabotage
Förändring av data
Vandalism
Stöld
Bombhot
Obehörigt röjande av hemligheter
Industrispionage
Krig
Oavsiktliga misstag
Mänskliga misstag och försumligheter
Vårdslöst yppande
Felbedömningar av ledningen
Adminsitrativa misstag
Tekniska
Bränder
Strömavbrott
Hård- och mjukvarufel
Olyckor
Miljöbetingade
Blixtnedslag
Stormar och orkaner
Översvämning
Elektriska störningar
Extrema temperaturer

Hotaktörer cybersäkerhet (antagonistiska)

National-stater

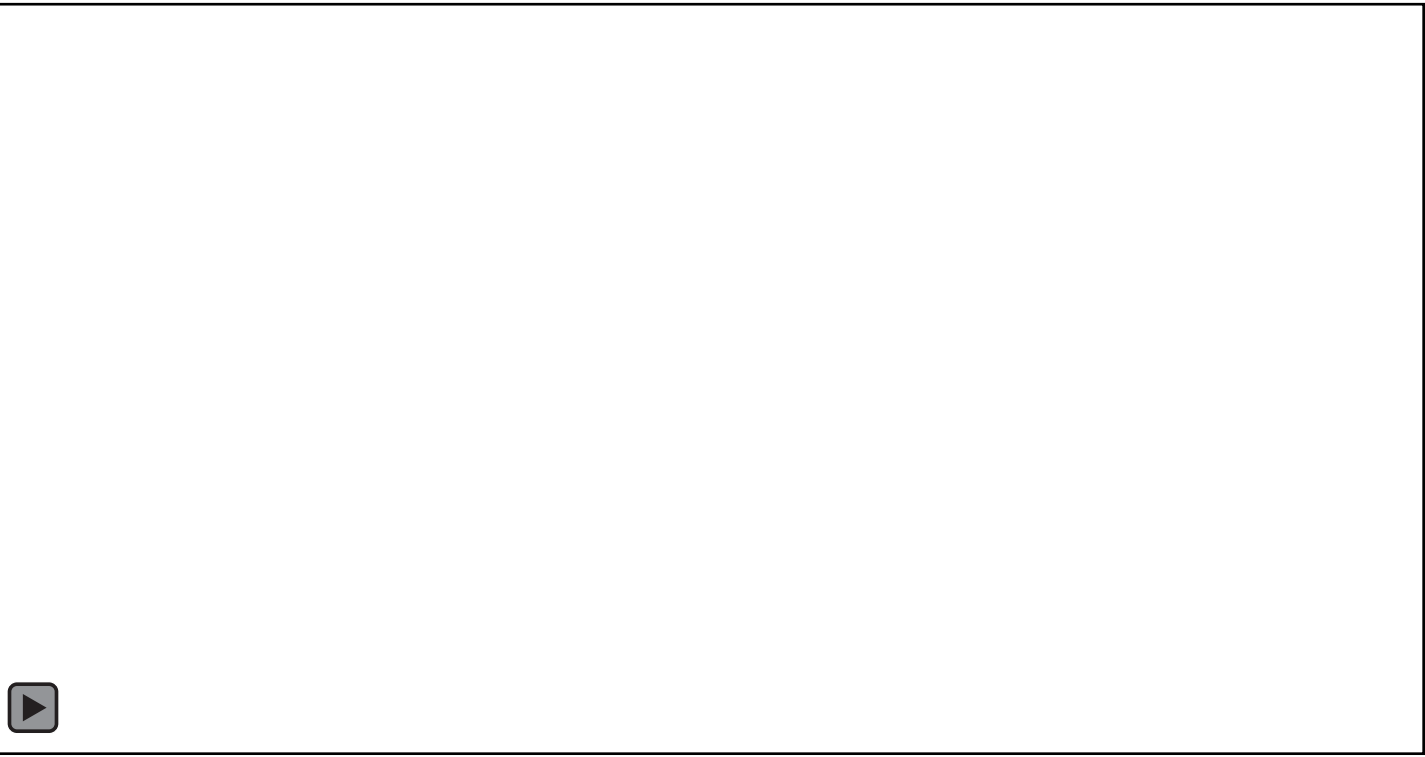
Hacktivister

INSIDER!

Cyber-terrorister

Organiserad brottslighet

Pågående cyberattacker enligt www.norsecorp.com

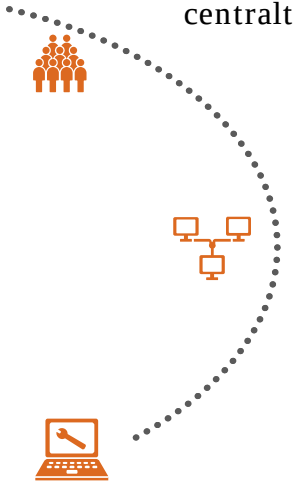


Nästa steg: Bygg upp rätt nivå på säkerheten

GDPR som drivare och möjliggörare av ordning och reda

Allt hänger ihop

Registerförteckning
Informationstexter
Laglig Grund – Principer
Gallring
Registerutdrag



Etablering av roller och ansvar är centralt för att säkerställa efterlevnad

Standardiserade processer implementeras för att möjliggöra en helhetssyn

Systemstöd för att möjliggöra informationshantering

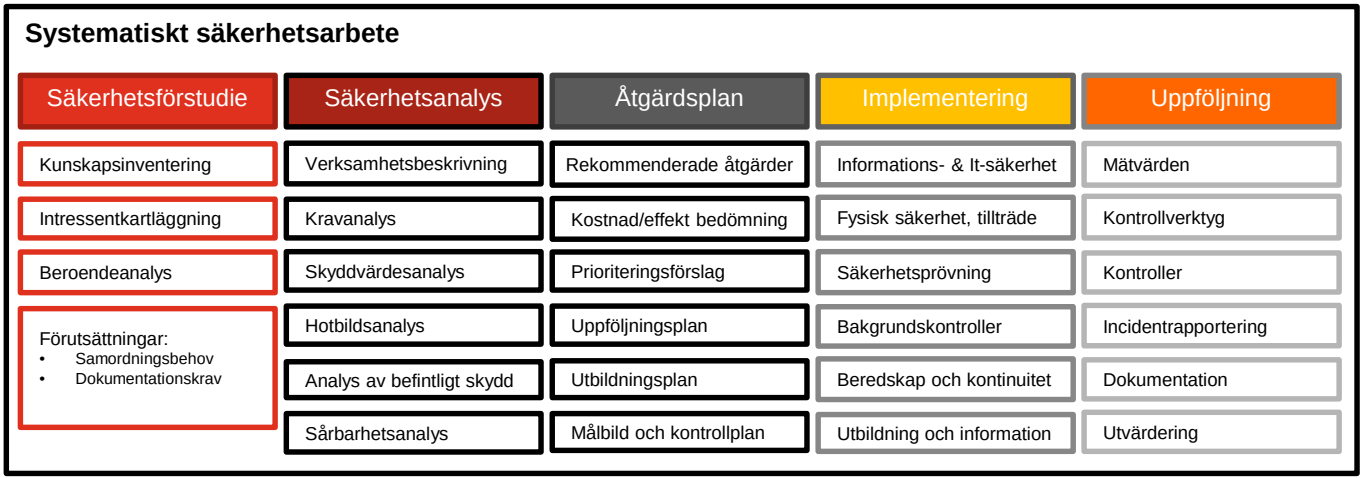
Elementära it-säkerhetsfunktioner för att kunna leva upp till kraven i dataskyddsförordningen

Exempel på säkerhetsåtgärder som bör vara implementerade

- Informationsklassificering
- Changemanagement
- Säker systemkonfigurering
- Nätverkssegmentering
- Behörighetsstyrning
- Accesskontroll
- Kryptering
- Dataläckageskydd
- DDOS-attackskydd
- Användaraktivitetsövervakning
- Logghantering/-analys
- Sårbarhetshantering
- Incidenthantering
- Krisberedskap

Systematiskt säkerhetsarbete

Analysen genomförs i fem steg och anpassas efter behov



Fördelar med ett GDPR-genomförande

Extern fördel – Ökat kundförtroende och ökade marknadsandelar (nivå 3)

GDPR-arbetet medför att kunderna känner att organisationen hanterar deras personuppgifter på ett ytterst professionellt sätt och vågar förlita sig på organisationen för ett närmare samarbete eller kund- och leverantörsrelation.

Intern fördel – Robust it-säkerhet och verksamhet (nivå 2)

Med ett väl avvägt GDPR-genomförande har organisationen höjt sin it-säkerhetsnivå så att verksamheterna är bättre rustade att motstå antagonistiska angrepp och it-kollapser (icke-antagonistiska händelser).

Legal fördel – Regelefterlevnad (nivå 1)

Inte bryta mot lagen.

Undvika sanktioner.

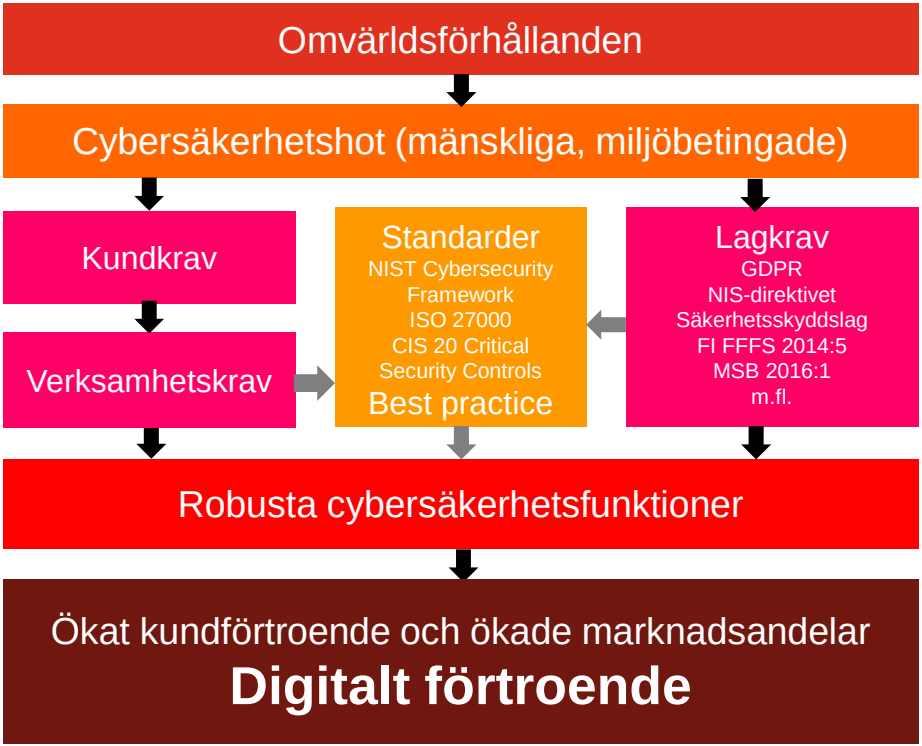
Nivå 3
Ökat kundförtroende och ökade marknadsandelar

Nivå 2
Robust it-säkerhet och verksamhet

Nivå 1
Regelefterlevnad

Vägen fram till att förtjäna förtroende

Förändrade omvärlds-förhållanden, ökande cybersäkerhetshot, höjda lag-, kund- och verksamhetskrav leder alla fram till behovet av effektiva cybersäkerhets-åtgärder, som skall öka kundernas förtroende och som skickligt utfört ger ökande marknadsandelar, vilket leder till ett **digitalt förtroende**.



Tack!

Kontakt

Mats Kellqvist
076 – 765 57 78
mats.kellqvist@pwc.com