

Cybersikkerhed og leverandørstyring

maj 2022



Agenda

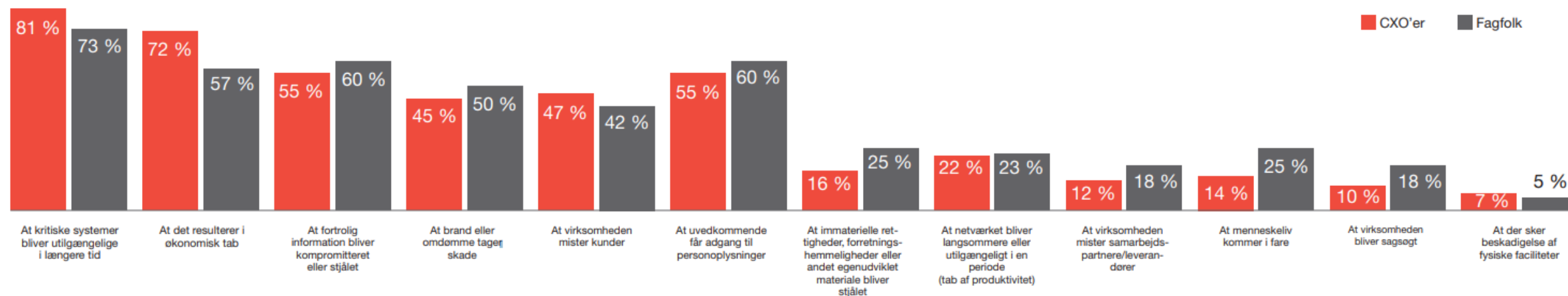
1. Hvad er vi bange for?
2. Processen
3. Cybersikkerhed i kontrakter med eksempler fra andres ulykker

Hvad er vi bange for?



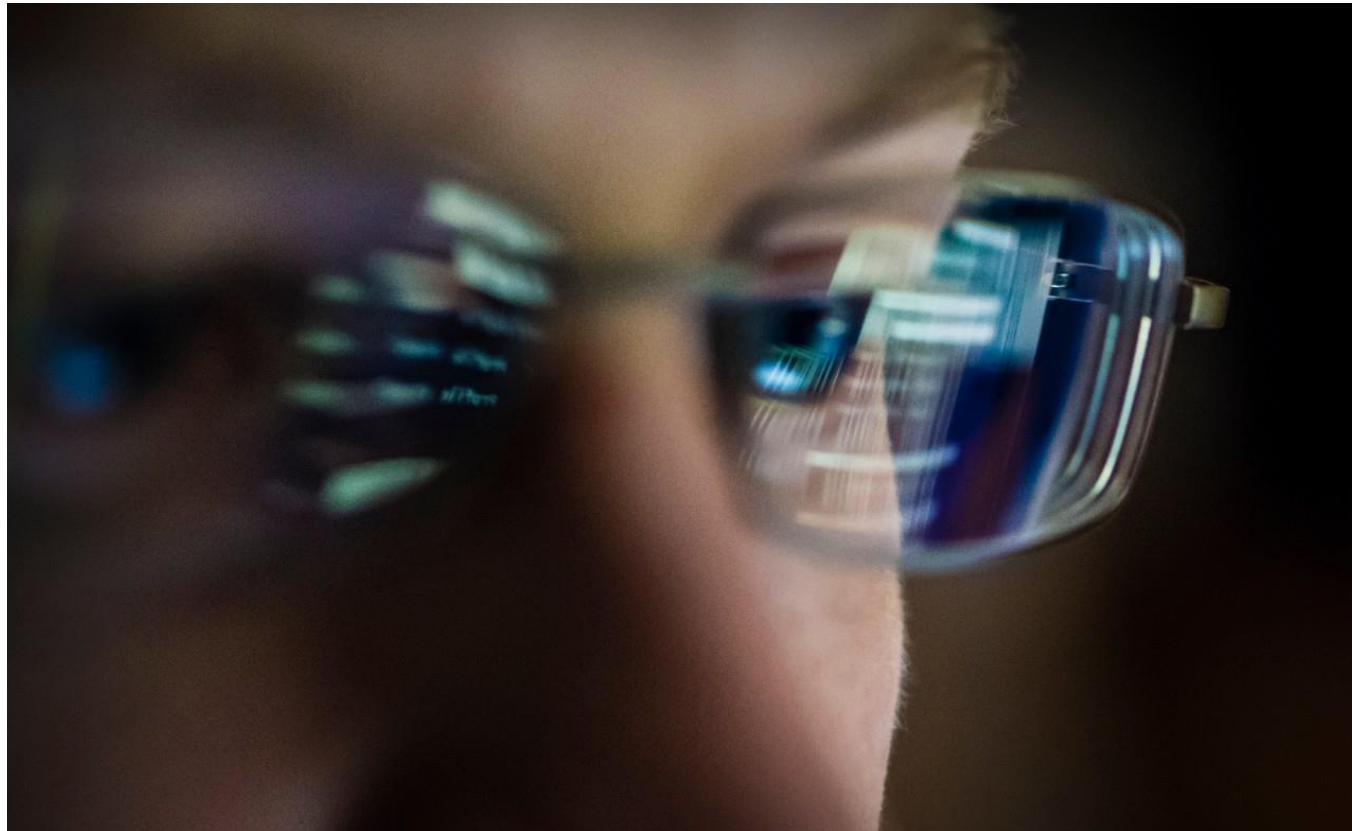
Utilgængelighed er topscorer

Hvad er din virksomheds største bekymring i relation til konsekvenserne af en cyberhændelse?



KILDE: <https://www.pwc.dk/da/publikationer/2021/cybercrime-survey-2021.html>

Tab af tilgængelighed – hacker eller en uheldig change ?

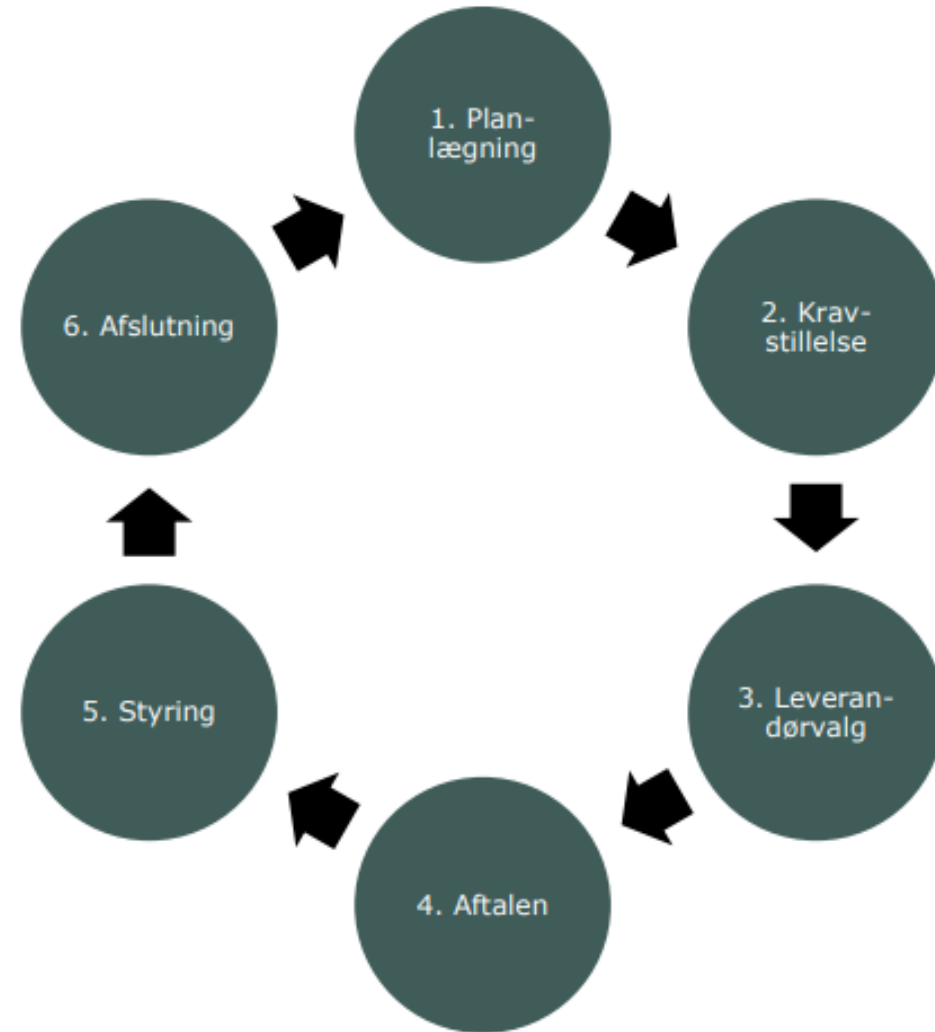


Processen

Erhvervsorganisations cyber- og informationssikkerhed
Består af tre elementer:

1. **Personer**
2. **Processer**
3. **Teknik**

- Opretholdelse af cyber- og informationssikkerhed er en PROCES – ikke en engangsinvestering.
- Cyber- og informationssikkerhed er 80 % organisation og 20 % teknik
- Trapper vaskes fra oven – Ledelsen sætter retning



Kilde: https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/Vejledning-cybersikkerhed-i-leverandorforhold_cfsc_digst-2022.pdf

Cybersikkerhed i kontrakter D17 (afsnit 10)

D17 forudsætter

- Bilag 4b (Sikkerhedskrav)
- Kunden har interne sikkerhedsforskrifter

Lige omkring sikkerhedskrav:

”Trappen skal sikres mod umiddelbar adgang”



Leverandørens egne ændringer (afsnit 10.3)

Leverandørens ændringer af sikkerhedsforanstaltninger, der ikke er kundespecifikke, men foretages som led i tilpasning til overholdelse af God it-skik og generelle sikkerhedsforskrifter gældende samlet for flere af Leverandørens kunder, sker for Leverandørens egen regning og håndteres som en ændringsanmodning fra Leverandøren efter pkt. 27.2.

Til overvejelse:

Hvem er de relevante parter i egen organisation som skal sige ok til ændring fra leverandøren?

Er det "kun" en teknologisk beslutning eller er der forretningsmæssige overvejelser? (fx freeze)

Antivirus og beskyttelse mod hacking (afsnit 10.4)

Leverandøren anvender tidssvarende, opdaterede og dokumenterede beskyttelsesforanstaltninger mod virus- og hacker-angreb i overensstemmelse med God it-skik i branchen, herunder alment accepterede standarder og retningslinjer

Til overvejelse:

Hvad er forventningen ? ClamAV ? Defender? Red Canary ? OpSwat?

Dækningsgrad og rapportering ? Opdateringsfrekvens ? ("AV rapporterer 95 % opdateret").

Hvem beslutter hvad der ikke skal AV på ? (Installeret vs aktiv)

Beredskabsplaner og back-up (afsnit 10.5)

Leverandøren skal opretholde systemer, procedurer og aftaler, der sikrer back-up i henhold til Bilag 4b (Sikkerhedskrav).

Leverandøren skal én gang årligt dokumentere overfor Kunden, at beredskabet er blevet testet og fungerer i overensstemmelse med beredskabsplanen. (Uddrag)

Til overvejelse:

Backup uden restore er intet værd. Restore tager tid!! (enkelt fil ? , enkelt server ? , "bare metal"-recovery ?)

Hvordan vil du som KUNDE indgå i beredsskabsafprøvning? – Egen plan for forretningskontinuitet ?

Sikkerhedshændelser (afsnit 10.6)

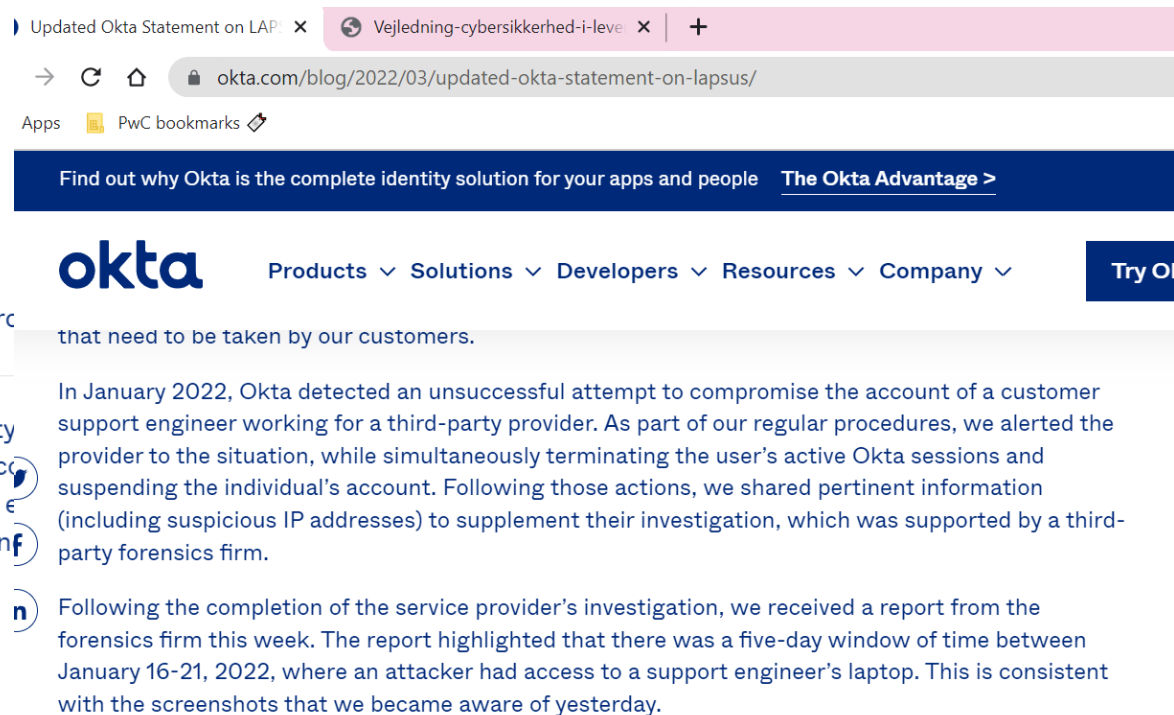
Leverandøren skal reagere på Sikkerhedshændelser, når Leverandøren bliver bekendt hermed, og i øvrigt tage initiativet til at sikre en hensigtsmæssig håndtering heraf i overensstemmelse med God it-skik, hvilket eksempelvis omfatter... (Uddrag)

Til overvejelse: Leverandørens leverandører?



Okta

In late January 2022, Okta detected an attempt to compromise the account of a third party support engineer working for one of our subprocessors. The matter was investigated and connected to the subprocessor. We believe the screenshots shared online are connected to this January event. Based on our investigation to date, there is no evidence of ongoing malicious activity beyond the activity detected in January.



Updated Okta Statement on LAPS

okta.com/blog/2022/03/updated-okta-statement-on-lapsus/

Find out why Okta is the complete identity solution for your apps and people [The Okta Advantage >](#)

okta Products Solutions Developers Resources Company Try Okta

that need to be taken by our customers.

In January 2022, Okta detected an unsuccessful attempt to compromise the account of a customer support engineer working for a third-party provider. As part of our regular procedures, we alerted the provider to the situation, while simultaneously terminating the user's active Okta sessions and suspending the individual's account. Following those actions, we shared pertinent information (including suspicious IP addresses) to supplement their investigation, which was supported by a third-party forensics firm.

Following the completion of the service provider's investigation, we received a report from the forensics firm this week. The report highlighted that there was a five-day window of time between January 16-21, 2022, where an attacker had access to a support engineer's laptop. This is consistent with the screenshots that we became aware of yesterday.

Sikkerhedsbrud (afsnit 10.7)

Konstaterer Leverandøren et brud på persondatasikkerheden omfattet af Databeskyttelsesforordningens art. 33, skal Leverandøren uden unødigt forsinkelse, og i øvrigt i overensstemmelse med art. 33, underrette Kunden herom. Dette gælder også, selvom sikkerhedsbruddet er afhjulpet, og de berørte personoplysninger ikke er blevet kompromitteret.

Til overvejelse:

Kan du selv klassificere hændelsen og reagere i tide?

Afslutning

Erhvervsorganisations cyber- og informationssikkerhed
Består af tre elementer:

1. **Personer**
2. **Processer**
3. **Teknik**

- Opretholdelse af cyber- og informationssikkerhed er en PROCES – ikke en engangsinvestering.
- Cyber- og informationssikkerhed er 80 % organisation og 20 % teknik
- Trapper vaskes fra oven – Ledelsen sætter retning

Indtænk STYRING
af kontrakt og
rapportering fra leverandør:

Det kræver dedikerede ressourcer

Kontakt

Thomas Kristmar

PwC | Director, Cyber Security

M: +45 5087 9661

E: thomas.kristmar@pwc.com

www.pwc.dk

Succes skaber vi sammen ...

Denne publikation er udarbejdet alene som en generel orientering om forhold, som måtte være af interesse, og gør det ikke ud for professionel rådgivning. Du bør ikke disponere på baggrund af de oplysninger, der er indeholdt i denne publikation, uden at indhente specifik professionel rådgivning. Vi afgiver ingen erklæringer eller garantier (udtrykkeligt eller underforstået) hvad angår nøjagtigheden og fuldstændigheden af de oplysninger, der findes i publikationen, og, i det omfang loven tillader, accepterer eller påtager PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, dets aktionærer, medarbejdere og repræsentanter sig ikke nogen forpligtelse, ansvar eller agtpågivenhedspligt for eventuelle konsekvenser, som følger af, at du eller andre handler eller undlader at handle i tillid til de oplysninger, der findes i publikationen, eller for eventuelle beslutninger truffet på baggrund af publikationen.

© 2022 PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab. Alle rettigheder forbeholdes. I dette dokument refererer "PwC" til PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, som er et medlemsfirma af PricewaterhouseCoopers International Limited, hvor hver enkelt virksomhed er en særskilt juridisk enhed.