TRUESEC

wtw

WTW Cyber Defender

WTW

WTW er Danmarks største uvildige forsikringsrådgiver med mere end 35 års erfaring på det danske marked og har i dag over 400 medarbejdere på kontorer i hele landet. WTW har lokale og globale eksperter i cyberforsikring og kan skræddersy forsikringsprogrammer til virksomheder i alle brancher. WTW bistår desuden med råd og vejledning i skadesager og varetager virksomhedens interesser over for forsikringsselskabet.

Cybersikkerhed er blevet et helt centralt fokusområde

Cybertruslen mod danske virksomheder er meget høj. Det vurderer det danske Center for Cybersikkerhed. Antallet af virksomheder, der bliver udsat for cyberangreb og andre former for brud på datasikkerheden, har da også været stærkt stigende i de senere år – og konsekvenserne for de virksomheder, der bliver ramt, er alvorlige og medfører ofte omkostninger i millionklassen i mistede indtægter og udgifter til genetablering af driften.

Alvoren er da også gået op for mange virksomheder, der har gjort cybersikkerhed til et helt centralt fokusområde og gjort en målrettet indsats for at øge it-sikkerheden. Det er en vigtig indsats, der er med til at afværge mange angreb, men desværre udvikler de cyberkriminelle hele tiden nye og mere sofistikerede metoder til at bryde ind i virksomhedernes it-netværk og bliver løbende bedre til at identificere følsomme data, som de enten krypterer eller truer med at offentliggøre, medmindre virksomheden betaler en betragtelig løsesum.

Det konstante pres fra mere eller mindre velorganiserede hackergrupper fra det meste af verden stiller store krav til enhver virksomhed om at skabe og fastholde et højt cybermæssigt sikkerhedsniveau – og om at have de fornødne processer og den rette forsikringsdækning til håndtering af brud på datasikkerheden.

Truesec

Truesec er en global cybersikkerhedsvirksomhed, der er på forkant med at beskytte organisationer og samfund mod cybertrusler. Truesecs formål er at skabe sikkerhed og bæredygtighed i en digital verden ved at forhindre cyberbrud og minimere dets påvirkning. Truesecs mere end 150 cyberspecialister dækker hele spektret af cybersikkerhed og hjælper dagligt virksomheder med at forsvare deres mest værdifulde dataaktiver.

WTW Cyber Defender

Truesec er ekspert i cybersikkerhed. WTW er ekspert i cyberforsikring. Vi har kombineret vores styrker og har skabt WTW Cyber Defender, der består af seks delelementer, som hver især er med til at styrke virksomhedens cybersikkerhed, og som samlet set giver de bedste forudsætninger for at forebygge skader og undgå tab på grund af brud på datasikkerheden.

WTW Cyber Defender dækker hele spektret fra forebyggelse over forsikring til krisehåndtering, hvor Truesec og WTW hver især byder ind med deres særlige ekspertise, og WTW Cyber Defender bidrager dermed både til at reducere risikoen for et cyberangreb og til at begrænse konsekvenserne.

Som kunde er I velkomne til at udvælge de delelementer, der giver mening for jer som virksomhed, og I vil i alle tilfælde opleve at blive vejledt af nogle af markedets mest erfarne rådgivere og specialister.

Kontakt WTW via e-mail på cyberdefender@willistowerswatson.com, og få mere at vide om, hvordan WTW Cyber Defender kan skabe større cybersikkerhed for jeres virksomhed.

WTW Cyber Defender – Elementer

wtw
Forsikringsanalyse

WTW udfører en grundig analyse af virksomhedens behov for cyberforsikring.

Prisen er individuel og aftales med WTW.

TRUESEC
Risikoanalyse

Truesec udfører en omfattende analyse af virksomhedens eksponering over for brud på datasikkerheden.

Der er fire modeller, som står nærmere beskrevet på næste side.

TRUESEC
Risikorådgivning

Truesec rådgiver om forebyggende tiltag, der reducerer risikoen for cyberangreb og begrænser konsekvenserne af et brud på datasikkerheden.

Prisen er individuel og aftales med Truesec.

wtw
Cyberforsikring

WTW gennmfører et udbud af virksomhedens cyberforsikring og udvælger det forsikringsselskab, der kan tilbyde de bedste betingelser til den mest attraktive pris.

TRUESEC
Krisehåndtering

Truesec sætter de fornødne foranstaltninger i værk for at standse angrebet, når der sker et brud på datasikkerheden, og aktiverer de relevante ressourcer for at sikre en hurtig genetablering af driften.

wtw
Skadehåndtering

WTW bistår med råd og vejledning, når der opstår skader, og varetager virksomhedens interesser i dialogen med forsikringsselskabet.

Kom databruddet i forkøbet

Truesec – Risikoanalyse

Truesec stiller sin unikke ekspertise og erfaring med databrud og cyberkriminalitet til rådighed for virksomheder, der ønsker at skabe sikre netværk og systemer, via grundige analyser af virksomhedens it-systemer og -processer.

Truesecs risikoanalyser giver indblik i virksomhedens eksponering over for brud på datasikkerheden og skaber et kvalificeret grundlag for prioritering af indsatsområder og minimering af risici. Der findes fire forskellige risikoanalyser, der i dybde og bredde er nøje tilpasset virksomhedens størrelse og it-mæssige kompleksitet.

På næste side kan du se et diagram og læse mere om de 14 delelementer, der indgår i den komplette analyse.

Truesec – Risikoanalyser	Mikro	Lille	Mellem	Komplet
Målgruppe	Små virksomheder	Små virksomheder	Små, mellem og store virksomheder	Mellem og store virksomheder
Format	Virtuelt	Onsite / Virtuelt	Onsite / Virtuelt	Onsite / Virtuelt
Varighed	1 dag	2 dage	5 dage	8-10 dage
Resumé	Truesec benytter en interviewbaseret tilgang til at foretage en struktureret risikovurdering af virksomheden. Som led i analysen, vil vi identificere det nuværende trusselsbillede for den respektive virksomhed og kortlægge virksomhedens modstandsdygtighed over for cyberangreb.	Truesec udbygger risikovurderingen ved at gennemføre en række tekniske tests af blandt andet virksomhedens brugerstyringssystem. De tekniske tests skal bruges til at kortlægge den faktiske modstandsdygtighed i virksomhedens absolutte it-kerne.	Truesec gennemgår i samarbejde med virksomheden de kritiske cybersikkerhedsforsvarsområder. Som led i denne analyse vil vi gennemføre en trusselssimulering for at kunne identificere en angribers vej igennem jeres virksomhed. Dermed kan vi præcist prioritere, hvor og hvordan vi kan styrke jeres forsvar.	Truesec gennemgår i samarbejde med virksomheden det konkrete cybersikkerhedsniveau for hele virksomhedens angrebsflade. Denne øvelse inkluderer dermed også gennemgang af jeres Office 365-miljø samt eventuelle cloud-miljøer. Den komplette analyse vil give jer tydeligt indblik i jeres konkrete modstandskraft.
1. Generel risikovurdering	✓	✓	✓	✓
2. Sårbarhedsanalyse	✓	✓	✓	✓
3. Active Directory-analyse	✓	✓	✓	✓
4. Endpoint Detection and Response-modenhedsvurdering		✓	✓	✓
5. Netværksanalyse		✓	✓	✓
6. Backup-vurdering		✓	✓	✓
7. Analyse af tredjepartsintegration			✓	✓
8. Insurance Baseline-analyse			✓	✓
9. Advanceret trussels- og angrebssimulering			✓	✓
10. Cloud-sikkerhedsanalyse: Azure, AWS, Digital Ocean etc.			✓	✓
11. Anti-virus / Malware / EDR-systemafprøvning				✓
12. Netværksarkitektur, segmentering og isolation				✓
13. Analyse af procedure for deling af ressourcer, fildrev m.m.				✓
14. Office 365-sikkerhedsanalyse				✓

Truesec – Riskoanalyse

1 **Generel risikovurdering**

En risikovurdering benyttes til at sikre prioritet og fokus på virksomhedens cybersikkerhedstiltag. Når risikoen kendes, kan fremtidige tiltag prioriteres.

2 **Sårbarhedsanalyse**

Alle systemer vil over tid forældes. Det er vigtigt at holde styr på disse systemer og services, så de ikke medvirker til sikkerhedsbrud.

3 **Active Directory Analyse**

Medarbejdere og services benytter typisk Active Directory eller Azure AD til at styre adgangen til virksomhedens it-systemer. Kompromitteres dette system, kompromitteres hele virksomheden.

4 **Endpoint Detection and Response (EDR)-modenhedsvurdering**

Det er vigtigt, at virksomheden er i stand til at opdage og stoppe eventuelle angreb. Angribere efterlader sig spor, og de spor skal opdages.

5 **Netværksanalyse**

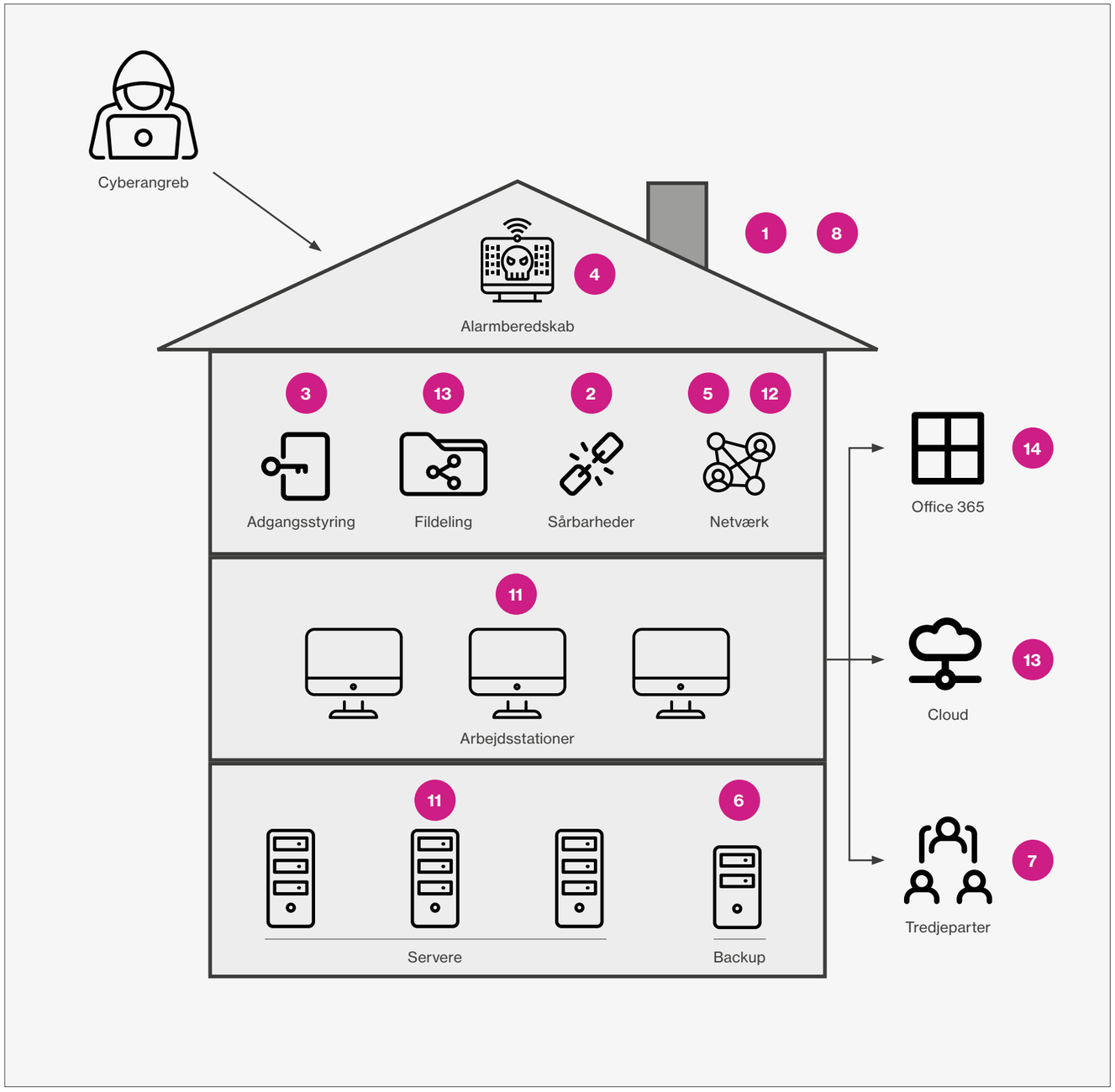
Netværket er nøglen til kommunikation mellem alle systemer og services i virksomheden. Begrænses adgangen til virksomhedens forskellige netværk, vil det gøre livet svært for en hacker.

6 **Backup-vurdering**

I tilfælde af en it-brist er det vigtigt for virksomheden at kunne gendanne de vigtigste services meget hurtigt.

7 **Vurdering af tredjepartsintegration**

Tredjeparts-virksomheder benyttes ofte til at drifte, udvikle og vedligeholde interne it-systemer. Det betyder også, at kompromittering af tredjeparter kan betyde kompromittering af virksomhedens systemer.



8 **Insurance Baseline-analyse**

WTW og Truesec har udviklet et rammeværktøj til vurdering af en række udvalgte cybersikkerheds-domæner.

9 **Avanceret trussels- og angrebssimulering**

En trusselssimulering gør det muligt præcist at se og forhindre de veje, som en hacker vil benytte igennem jeres virksomhed.

10 **Cloud-sikkerhedsanalyse: Azure, AWS, Digital Ocean**

Skyen gør it-infrastruktur tilgængeligt og skalerbart, men det betyder også, at virksomhedens infrastruktur pr. definition er online, og beskyttes den ikke korrekt, kan det blive fatalt.

11 **Anti-Virus / Malware / EDR-systemafprøvning**

Det er vigtigt, at virksomheden aktivt holder øje med sikkerhedshændelser, og at programmer fintunes til detektering. Ofte har virksomheden implementeret overvågningsudstyr, men ingen opdager de alarmer, der genereres.

12 **Netværksarkitektur, segmentering og isolering**

Praktisk afprøvning af jeres netværksarkitektur og implementering vil sikre, at forventningen stemmer overens med virkeligheden.

13 **Analyse af procedure for deling af ressourcer, fildrev**

Fildeling er nødvendig i alle virksomheder, men det er lige så nødvendigt at sikre, at ingen har uretmæssig adgang til følsom persondata eller lignende igennem eksempelvis fildrev.

14 **Office 365-sikkerhedsanalyse**

E-mail, Office m.m. Det er alt sammen kritiske virksomhedsressourcer, og derfor indeholder de ofte meget kritisk information, der hurtigt bliver tilgængeligt online, hvis ikke de sikres.

cyberdefender@willistowerswatson.com

Nærum
Rundforbivej 303
2850 Nærum
+45 8813 9600

Aarhus
Tangen 17
8200 Aarhus N
+45 8813 9400

Holstebro
Nupark 49F
7500 Holstebro
+45 8813 9400

Aalborg
Østre Havnepromenade 24
9000 Aalborg
+45 8813 9200