FINANS
DANMARK

8 initiativer der kan styrke cybersikkerheden i Danmark

November 2017


Historik
Bogmærker
Personer
Vindue
Hjælp
www.investing.com/charts/multiple-indices-streaming-charts
Sign In / Sign up
Markets
News
Analysis
Charts
Technical
Social Trading
Brokers
Tools
Portfolio
Alerts
More
Live Charts
Forex Chart
Futures Chart
Stocks Chart
Indices Chart
Multiple Forex Charts
Multiple Indices Charts
EUR/USD or AAPL
S&P 500, United States, 5, N...
realtime
Investing.com
Dow Jones Industrial Average...
DAX, Germany, 5, Xetra (CF...
FTSE 100, United Kingdom, 5...

Gør cybersikkerhed til en dansk styrkeposition

Danmark er et af de mest digitaliserede lande i verden. Digitaliseringen har skabt vækst og udvikling i hele landet til gavn for borgere, virksomheder og det offentlige. Men det gør os også sårbare over for cyberangreb. Cybertruslen er reel, og den er øget betragteligt i de seneste år, så der i dag er en meget høj trussel mod Danmark, særligt fra cyberspionage og -kriminalitet.

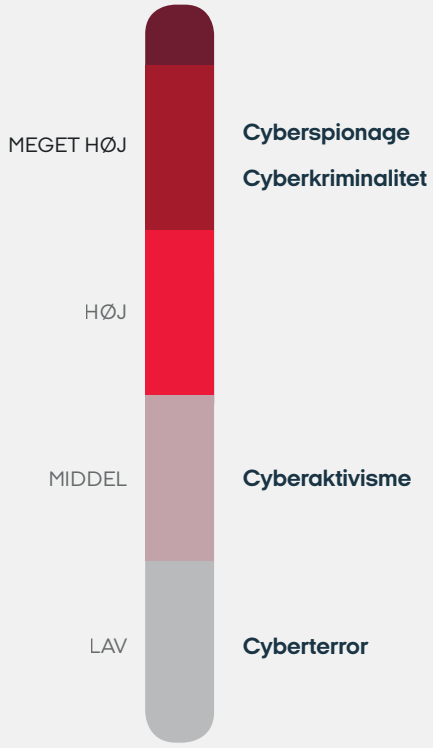
Borgere og virksomheder bliver dagligt hacket over hele verden. Det koster i dag op til 2 procent af BNP årligt i flere vestlige økonomier[1]. Borgerne oplever, at kriminelle forsøger at få adgang til deres penge og personlige oplysninger på nettet. Både danske og internationale virksomheder rammes af alvorlige angreb med store økonomiske tab til følge. Vi har set, hvordan hackere prøver at få indflydelse på demokratierne i de vestlige lande ved hjælp af cyberangreb og -spionage.

Dagsorden for digitaliseringen har været effektivisering og vækst, og der har været et mindre fokus på it-sikkerhed. Det bør vi ændre. Cybersikkerhed bør opprioriteres, og it-sikkerhed bør være en topprioritet for regeringen. Der skal handles nu, så tilliden til det digitale Danmark styrkes. Det vil være til gavn for hele Danmark og skabe et samfund rigere på muligheder.

Finans Danmark har 8 forslag til at styrke cybersikkerheden.

[1] Melissa Hathaway 2017

Trusselsvurdering mod danske myndigheder og private virksomheder



Kilde: Center for Cybersikkerhed, Forsvarsministeriet 2017

Op mod 1.000 gange om året bliver Danmark ramt af alvorlige hackerangreb fra fremmede statsmagter.

Kilde: Center for Cybersikkerhed, 2017

Danmark indtager en 34. plads på Global Cybersecurity Index 2017. Det er markant længere nede på listen end fx. vores nordiske naboer Sverige, Norge og Finland.

Kilde: FN-agenturet ITU, International Telecommunication Union, 2017

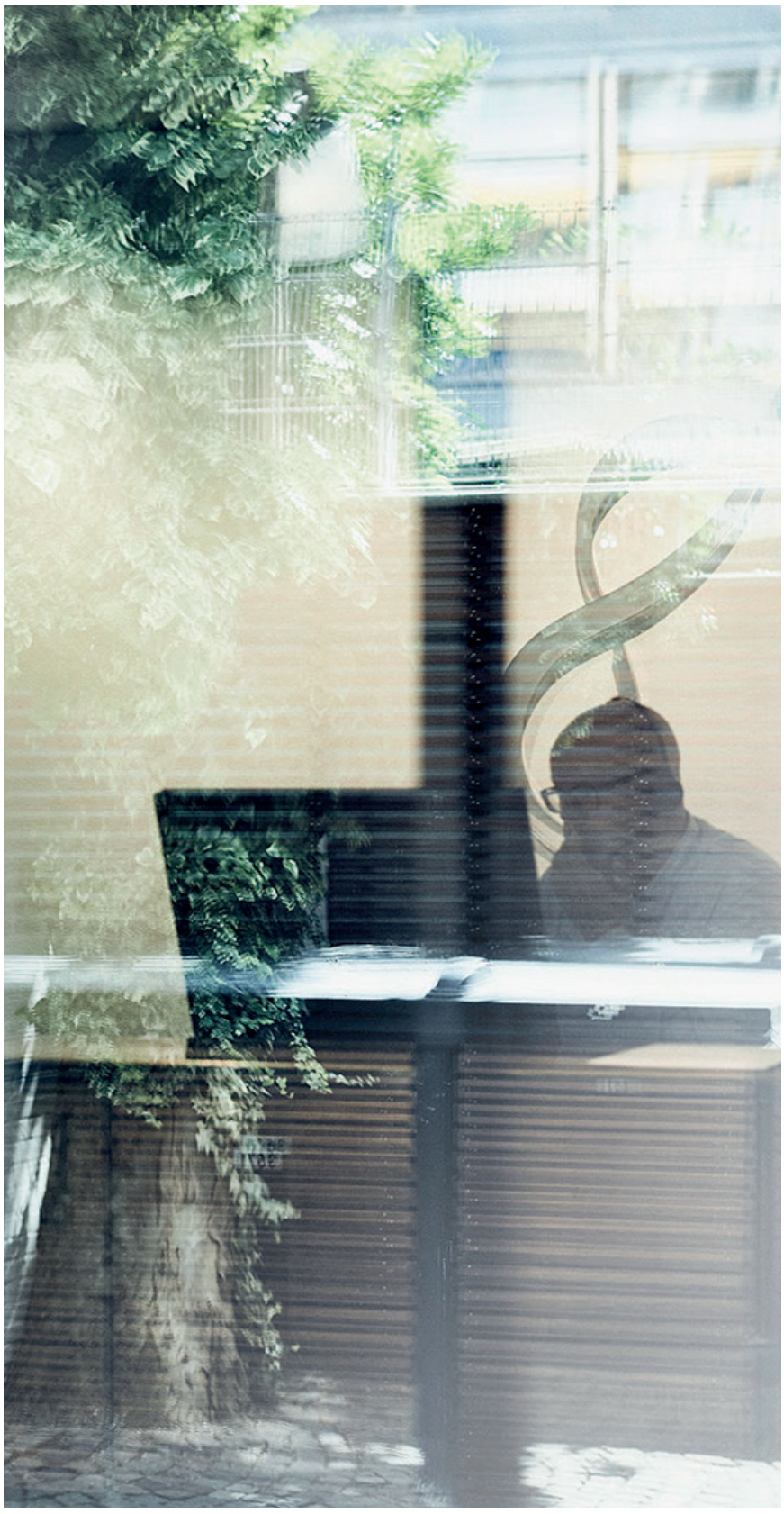
INITIATIV 1

Indtænk it-sikkerhed i visionen for det digitale Danmark

Danmark er i front, når det gælder digitalisering af samfundet, men vi er ikke det land, der har den bedste it-sikkerhed, og der er behov for en mere strategisk tilgang til it-sikkerhed. Det bør tænkes ind i al digitalisering. Der bør derfor gennemføres en strategisk cyberparatheds-vurdering af vores samlede it-sikkerhedsmodenhed på tværs af de politiske strategier for fx forsvaret, lovgivningen, håndhævelse samt forskning og udvikling. Formålet skal være at afdække, om it-sikkerhed er prioriteret tilstrækkeligt i forhold til visionen for udviklingen af det digitale Danmark.

En cyberparatheds-vurdering kan give et samlet billede af Danmarks prioriteringer på nationalt, regionalt og lokalt plan og udgøre en strategisk ramme til at afdække de fremtidige visioner og behov på området. Det kan f.eks. gøres med Cyber Readiness Index 2.0, som er en strategisk ramme til at vurdere et lands samlede cyberparathed. Flere lande har allerede udviklet en Cyber Readiness-landeprofil. Det gælder fx USA, Frankrig, Tyskland, Holland, Storbritannien, Italien og Japan.

Med afsæt i et Cyber Readiness Index eller lignende bør regeringen udarbejde en handlingsplan på de områder, hvor indekset viser, at der er et behov for en større indsats. Det skal ske i tæt samarbejde med erhvervslivet, så der både i det offentlige og det private skabes et stærkt forsvarsværk mod cyberangreb.



INITIATIV 2

En fælles digital indgang for virksomheders indberetning af it-sikkerhedshændelser til myndighederne

Det er for vanskeligt for virksomheder og borgere at gennemskue, hvordan de skal indberette cyberangreb og brud på it-sikkerheden. En hændelse skal indberettes til flere forskellige myndigheder, fx den lokale politikreds, Datatilsynet, sektormyndighed, Finanstilsynet og Center for Cybersikkerhed.

Finans Danmark foreslår, at der etableres en fælles digital indgang til indberetning af it-sikkerhedshændelser. Alle oplysninger om hændelserne skal opsamles i en fælles databank med henblik på at opbygge viden om cyberangreb og brud på it-sikkerheden.

Den centrale videnopsamling skal bruges til at forbedre forebyggelse hos virksomhederne, borgerne og myndighederne med henblik på at begrænse skaderne ved angreb.

INITIATIV 3

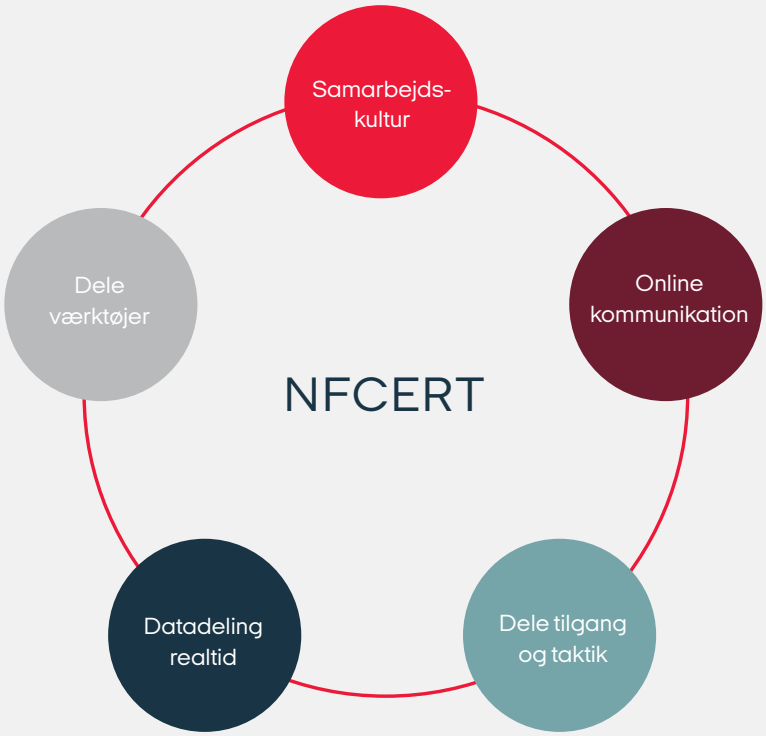
Proaktiv 24/7-rådgivning af virksomheder gennem øget datadeling.

Hurtig informationsspredning og sparring om hændelser er helt centralt for bekæmpelse af cyberkriminalitet. Der er mange forskellige myndigheder på området, men ingen har det samlede ansvar for den løbende proaktive videndeling og informationsindsats. Det er vanskeligt at få viden om aktuelle og konkrete hændelser og trusler, og de oplysninger, der er, må ofte ikke anvendes operationelt, fordi myndighederne klassificerer dem som fortrolige. Området er derfor præget af mørketal.

Der er behov for, at rådgivningen og videndelingen om cyberangreb styrkes i alle led, herunder mellem det offentlige og virksomhederne. Finans Danmark foreslår, at der etableres en fælles rådgivningsfunktion målrettet virksomheder. Den skal yde proaktiv rådgivning om konkrete hændelser, som er sket, og trusler, man står overfor. Det skal ske realtid og målrettes de enkelte sektorer. Rådgivningen skal blandt andet være baseret på de informationer, som opsamles gennem den foreslåede databank. Det kan fx ske via en webtjeneste eller en certificeringsordning for virksomheder.

Den finansielle sektor har etableret en fælles nordisk CERT [NFCERT] med henblik på at styrke forebyggelsen og videndelingen.

Finans Danmark vil gerne opfordre til, at andre sektorer overvejer muligheden for at etablere lignende fora. Det vil bidrage til at løfte it-sikkerheden generelt og styrke vækstmulighederne til gavn for hele samfundet.



Nordic Financial CERT og FSOR

Nordic Financial CERT [NFCERT] er et sektor samarbejde med deltagelse fra bl.a. banker, forsikingsselskaber og pensionsselskaber. Formålet er at styrke videndelingen om cyberaktiviteter.

Finanssektoren har etableret et sektorsamarbejde gennem Finansielt Sektorforum for Operationel Robusthed [FSOR], som er et samarbejdsforum mellem myndigheder og vigtige aktører i den finansielle sektor i Danmark.

Misbrug og svindel med betalingskort

Det økonomiske tab på kortmisbrug er tredoblet siden 2011. Det var i 2016 på godt 100 millioner kroner på Dankort.

jf. Nets

I 2014 blev 16.000 personer udsat for chikane på internettet i Danmark. Cikane kan være negative beskeder på sociale medier eller ændring af profil.

jf. facerape

INITIATIV 4

Borgerrettet information skal styrkes

Danske borgere udsættes hver dag for cyberangreb, hvor svindlere gennem internettet forsøger at berige sig selv økonomisk. Det kan fx være ved at få borgerne til at afgive deres kreditkort- eller netbankoplysninger. Eller det kan være ved gennem ransomware eller med falske fakturaer at få borgere og virksomheder til at betale til den it-kriminelle. Borgerne udsættes også i stigende grad for identitetstyveri og misbrug af personlige oplysninger som fx deling af private fotos eller misbrug af SoMe-profiler.

Der er i dag en række spredte danske offentlige og private initiativer for at styrke borgerne over for digital kriminalitet, men der mangler en mere permanent, løbende og systematisk indsats.

Rådgivningen og informationsindsatsen over for borgere kan med fordel styrkes væsentligt. Dette kunne ske gennem en central rådgivningsfunktion med borgerrettet information om it-sikkerhed og med rådgivning om, hvilke forholdsregler den enkelte kan træffe. Fx i form af en borgerrettet hjemmeside med løbende rådgivning, startpakker, kampagner m.m.

INITIATIV 5

En central politiindsats

Der er behov for, at politiet styrker indsatsen mod den cyberelaterede kriminalitet, særligt indenfor den økonomiske efterforskning, ved at man etablerer et stærkt center for cyberbekæmpelse. I dag er det de lokale politikredse, der i første omgang skal behandle henvendelser, men en cyberhændelse er ikke en lokal begivenhed. Den bør derfor ikke starte med en anmeldelse og efterforskning hos lokalbetjenten, men hos en eller to centrale enheder i politiet, som skal have ansvaret for cyberkriminalitet. Det vil styrke videndelingen på tværs af landet, styrke politiets kompetencer og have en positiv indflydelse på opklaringen af sager.

Endelig ønsker Finans Danmark, at der fortsat er et aktivt internationalt politisamarbejde om bekæmpelse af grænseoverskridende cyberhændelser. Derfor er det helt afgørende, at dansk politi sikres den bedst mulige adgang til Europolsamarbejdet.

PWC har spurgt ca. 350 virksomhedsledere, it-chefer og -specialister fra danske virksomheder om cyberkriminalitet.

77 %

har været udsat for phishing-angreb.

64 %

har været udsat for cyberangreb inden for det seneste år.

53 %

af de ramte virksomheder oplyser, at cyberangreb har haft økonomiske omkostninger.

Kilde: Cybercrime Survey 2017, PWC

INITIATIV 6

Træning af virksomhederne til at modstå cyberangreb

Det er vigtigt, at virksomhederne er parate til at modstå cyberangreb. For at teste evnen til at reagere på et cyberangreb er der behov for, at virksomhederne også jævnligt gennemfører test og øvelser. Træning i parathed overfor at reagere på cyberangreb er i dag en velintegreret del af det statslige beredskab på nationalt plan, fx i Den Nationale Operative Stab. Der er mange virksomheder, som i dag ikke har et tilstrækkeligt beredskabet, hvilket er et problem i forhold til at kunne afværge cyberangreb. Derfor bør der udvikles virksomhedsrelaterede øvelsespakker til træning i at reagere på cyberangreb.

1,5 mio. mails er blevet afvist siden implementering af DMARC 1. januar 2017 i Danske Bank.

Kilde: Danske Bank 2017

Det britiske skattevæsen har implementeret DMARC, og det har medført at 300 mio. phishingmails er fjernet årligt.

Kilde: HMRC 2016

INITIATIV 7

Bedre beskyttelse mod falske e-mails, SMS'er og websites

It-kriminelle retter i disse år i stigende grad indsatsen mod slutbrugerne. Redskabet er som oftest en sms eller en e-mail, som udgiver sig for at være andet og komme fra andre, end de i virkeligheden gør.

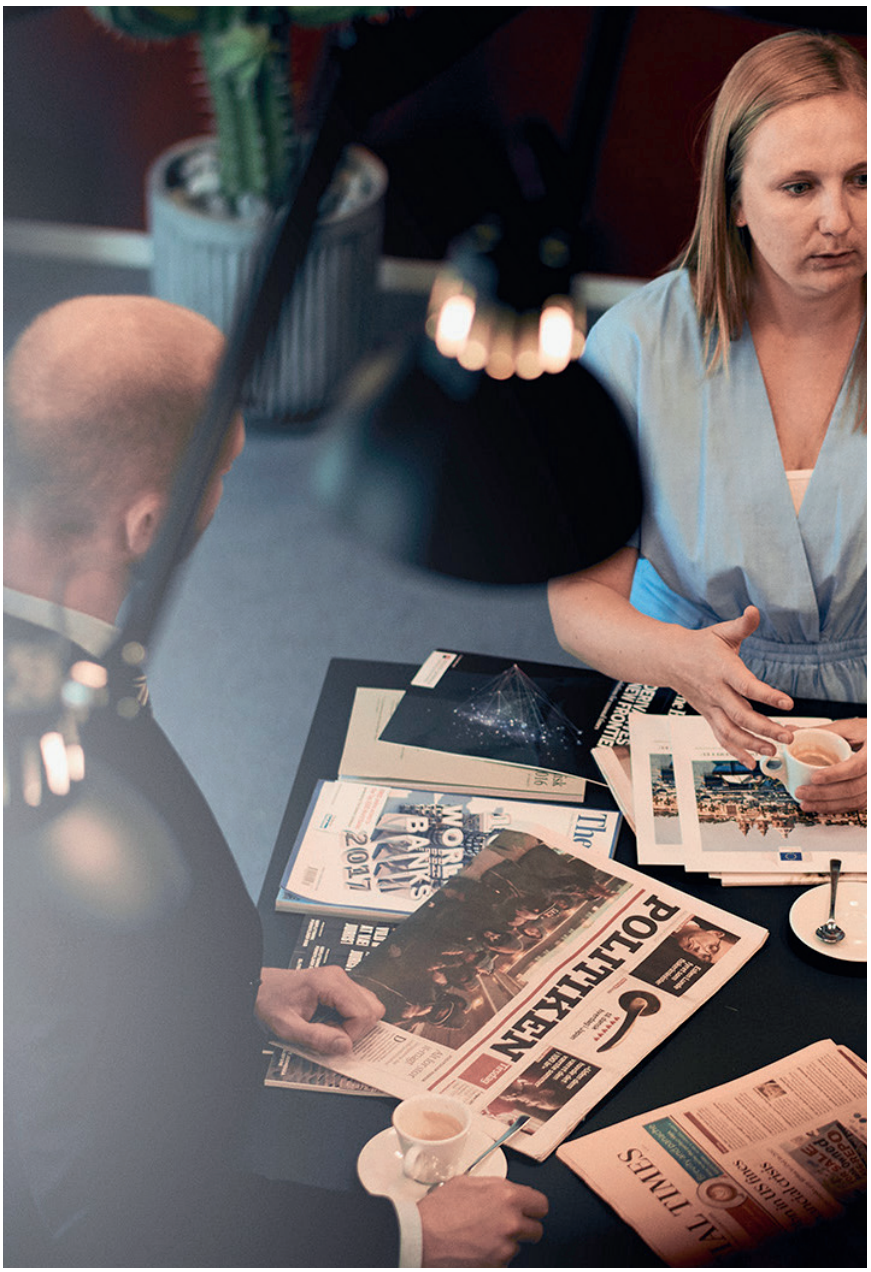
Tal for sektoren viser, at over 80 procent af de e-mails, som finansielle virksomheder modtager, er ondsindede og sendt af kriminelle (inkl. spammers). Der bør implementeres nye teknikker, der kan dæmme op for dette, fx DMARC[2] og DNSSEC[3], og filtrere falske e-mails væk.

Derfor bør der stilles krav om, at leverandører af samfundskritisk digital infrastruktur som udgangspunkt skal gå efter denne beskyttelse og i øvrigt hvor dette er relevant at tilbyde borgere beskyttelse i forbindelse med adgang til internettet. Endvidere bør offentlige myndigheder, som har megen digital borger- og virksomhedskontakt også implementere det. Derudover kan det være en betingelse ved anskaffelse af ny offentlig samfundskritisk digital infrastruktur. Det vil øge troværdigheden af de mails, der kommer fra det offentlige.

Endelig bør der ske et stærkere samarbejde på teleområdet, så vi også der får en løsning, der kan fange falske smsbeskeder, så de ikke glider gennem telenetværket.

[2] Domain-based Message Authentication, Reporting and Conformance

[3] Domain Name System Security Extensions (it-sikkerhedsfilter)



INITIATIV 8

Stærkere europæisk samarbejde om cybersikkerhed

EU-kommissionen har som følge af den seneste tids globale hackerangreb lanceret flere nye tiltag, der skal styrke it-sikkerheden i unionen.

Finans Danmark støtter tiltagene, herunder især et nyt EU-agentur for it-sikkerhed, der skal sikre bedre kommunikation landene imellem samt et forslag om fælles standard for it-sikkerhed. Det nye sikkerhedsagentur skal være en udvidelse af det allerede etablerede ENISA [The European Union Agency for Network and Information Security].

Det andet forslag er en EU-certificering i forhold til cybersikkerhed for produkter, der er koblet til internettet. På samme måde som fødevarer kan være EU-godkendte, skal produkter med internetadgang, som visse transportmidler, særlige biler og forbrugerprodukter også være det.

Finans Danmark støtter helt og fuldt de nye EU-initiativer. Cyberkriminalitet er grænseoverskridende, og det er afgørende, at vi i regi af EU har et stærkt europæisk værn mod cyberkriminelle. Det er samtidig vigtigt, at det internationale samarbejde ikke stopper ved Europas grænser.

8 initiativer

der kan styrke cybersikkerheden i Danmark

1 Indtænk it-sikkerhed i visionen for det digitale Danmark

2 En fælles digital indgang for virksomheders indberetning af it-sikkerhedshændelser til myndighederne

3 Proaktiv 24/7-rådgivning af virksomheder gennem øget datadeling.

4 Borgerrettet information skal styrkes

5 En central politiindsats

6 Træning af virksomhederne til at modstå cyberangreb

7 Bedre beskyttelse mod falske e-mails, SMS'er og websites

8 Stærkere europæisk samarbejde om cybersikkerhed

Finans Danmark – Amaliegade 7 – 1256 København K
Telefon 3370 1000 – www.finansdanmark.dk