CODANS

guide til it-sikkerhed

Hvad du som virksomhed bør vide om it-kriminalitet
og hvordan du kan forebygge det

CODAN

Indhold

Side 3.....Forord

Side 4.....Virksomhedernes tanker om it-kriminalitet

Side 5.....Sådan ser virkeligheden ud

Side 6.....Hvad gør virksomhederne for at undgå it-kriminalitet

Side 8.....Sådan forebygger I it-kriminalitet i jeres virksomhed

Side 10.....Hvis skaden skulle ske

Er I ordentligt sikret mod it-kriminalitet?

Mange virksomheder oplever i stigende grad at blive udsat for it-kriminalitet som virusangreb eller netbanksindbrud.

Faktisk har hver tiende mindre danske virksomhed inden for brancherne service, detail og håndværk ifølge vores tal været udsat for it-kriminalitet, og i mere end halvdelen af tilfældene er angrebet sket inden for det seneste år.

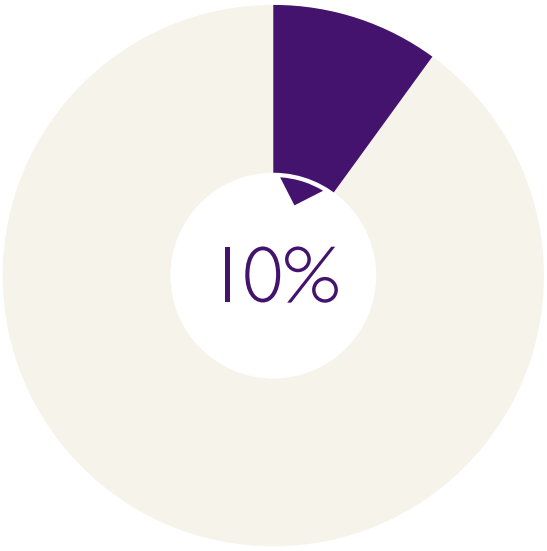
Selvom I måske ikke har mange servere, pc'er eller fortrolig data i jeres virksomhed, så kan I stadig være sårbare over for it-kriminalitet. Enten direkte, eller fordi nogen forsøger at bruge jer til at få ram på en virksomhed, som I er underleverandør til.

Og det kan være både tidskrævende og have alvorlige konsekvenser for jeres indtjening, hvis I bliver ramt af et virusangreb og mister jeres kundedatabase, eller hvis nogen bryder ind på netbankkontoen og stjæler måneders omsætning.

En forsikring mod it-kriminalitet er godt at have i sådanne tilfælde, men det er mindst lige så vigtigt at have sine sikkerhedsforanstaltninger i orden.

Derfor har vi i denne folder samlet fakta fra egne og andres undersøgelser af it-kriminalitet i mindre og mellemstore virksomheder samt en række gode råd til, hvad I kan gøre for at forebygge it-kriminalitet.

Anders Hestbech
Erhvervsdirektør
Codan Forsikring

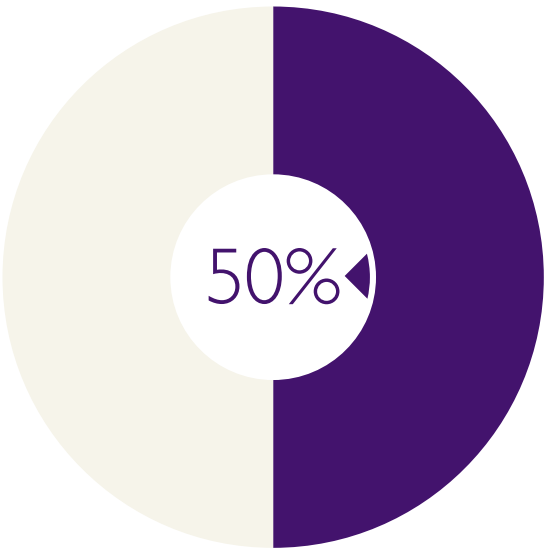


Kun 10 % af mindre danske virksomheder inden for brancherne, service, detail og håndværk bekymrer sig i høj grad om it-kriminalitet i det daglige[2]

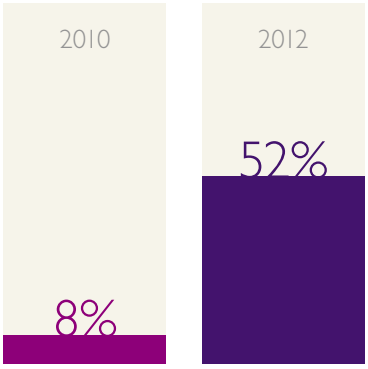
"Vi har ikke så meget it, så der er ikke så meget at bekymre sig om."

– Ansat i mindre virksomhed [1]

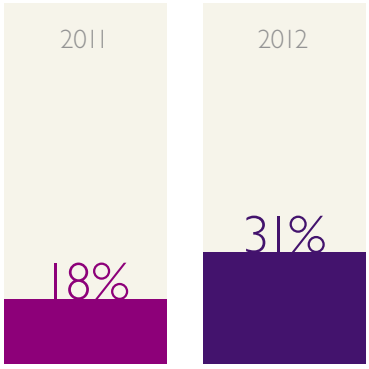
En global undersøgelse foretaget af Symantec blandt 1900 virksomheder med 5 til 499 ansatte viser, at halvdelen af disse virksomheder ikke regner med at blive ramt af hackere[3]



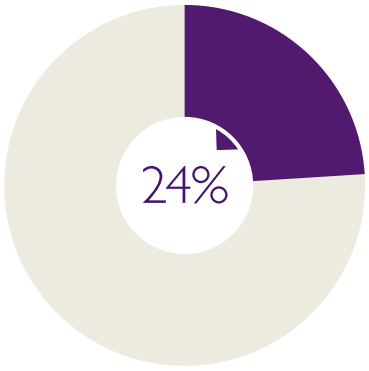
1 Citat fra Codans undersøgelse:
2 Undersøgelse blandt 232 mindre virksomheder (0-9 ansatte) udført af analyseinstituttet Wilke for Codan Forsikring, juli 2013
3 http://www.symantec.com/content/en/us/about/media/pdfs/symc-smb-threat-awareness-poll.pdf



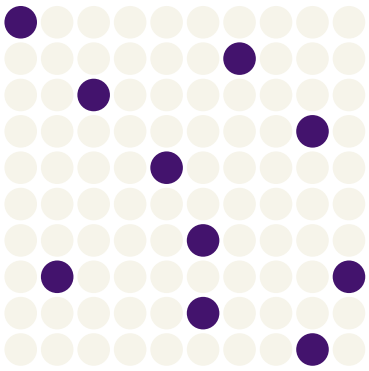
Private virksomheder har oplevet en eksplosiv stigning i antallet af angreb fra hackere. Blot 8 % af det samlede antal hackerangreb var rettet mod virksomheder i 2010, mens det tal i 2012 var steget til 52 % [4]



I 2012 var 31 % af alle målrettede hackerangreb rettet mod mindre og mellemstore virksomheder (op til 250 ansatte). I 2011 var det tilsvarende tal 18 % [5]



24 % af alle it-angreb i 2012 var rettet mod fremstillingsindustrien (produktionsvirksomheder, bygge og anlæg). Det gør den til den mest udsatte branche. Efterfulgt af finanssektoren (19 %) og servicesektoren (17 %) [5]



Hver tiende mindre danske virksomhed inden for brancherne service, detail og håndværk har været udsat for it-kriminalitet, og 60 % af tilfældene er sket inden for det seneste år [6]

I er en del af en større værdikæde

Målrettede angreb mod mindre virksomheder har ifølge it-sikkerhedsvirksomheden Symantec ofte til formål at ramme et andet mål – f.eks. en større virksomhed eller organisation, som den angrebne virksomhed er underleverandør til.

Så selvom I ikke har mange fortrolige data i jeres egen virksomhed, kan I stadig være sårbare over for it-kriminelle, der ønsker at bruge jeres it-systemer, som 'springbræt' til at få fat i vigtige informationer fra en af jeres kunder.

4 Ifølge en global undersøgelse fra KPMG. Se http://www.kpmg.com/DK/da/presserum/pressemeddelelser/pressemeddelelser2013/Sider/eksplosiv-stigning-i-hacking-mod-virksomheder.aspx
5 Symantec rapport: http://www.symantec.com/security_response/publications/threatreport.jsp
6 Undersøgelse blandt 232 mindre virksomheder (0-9 ansatte) udført af analyseinstituttet Wilke for Codan Forsikring, juli 2013

Det går jo egentlig meget godt

Eller hvad?

7. Undersøgelse blandt 232 mindre virksomheder (0-9 ansatte) udført af analyseinstituttet Wilke for Codan Forsikring, juli 2013

De fleste virksomheder har styr på installation af firewall, antivirus-software, opdatering og vedligehold af standardprogrammer.

Men mange glemmer de helt simple forholdsregler som daglig backup og løbende udskiftning af passwords.

Det går de it-kriminelle efter:

De it-kriminelle går generelt efter mange forskellige ting, men de er typisk ude efter data, som er bestilt, eller som de kan sælge videre til andre.

Data, som for eksempel e-mail adresser er interessante for de it-kriminelle fordi e-mail adresserne kan samles og sælges videre til andre, der har som levebrød at sende 'spam-mails'.

Interessant data kan for eksempel være:

- E-mail adresser
- Kreditkortoplysninger
- Anden personlig information
- Kunderegistre
- Kontaktdetaljer på ansatte og kunder
- Patenter og anden "Intellectual Property"
- Kontrakter, prislister osv.

Der er heldigvis en række simple forholdsregler, I som virksomhed kan tage for at reducere risikoen for it-kriminalitet.

DE TRE VIGTIGSTE RÅD

1 Brug et antivirusprogram med automatisk opdatering, en firewall og et anti-spywareprogram, og opdatér programmerne løbende

2 Opdatér jeres browsere og standardprogrammer som for eksempel Java, Adobe og Quicktime løbende. I kan tjekke status på programmerne på www.opdaterdinpc.dk

3 Tag sikkerhedskopi-/backup af virksomhedens data og systemer med faste intervaller, gerne dagligt

OBS!

De almindelige antivirusprogrammer fanger i dag kun ca. 50 % af alle virus eller malware angreb. Det kan derfor være en god idé at supplere en antivirusløsning med en såkaldt endpoint beskyttelse, der kan tilkøbes fra de fleste udbydere af it-sikkerhedsløsninger

Jeres egen adfærd er det vigtigste for en god it-sikkerhed

Når det kommer til it-sikkerhed, er det en god grundregel at opfordre alle virksomhedens medarbejdere til at bruge sin sunde fornuft – og bede dem spørge en it-kyndig, hvis de er i tvivl, eller opsøge en ekspert, hvis I oplever en konkret trussel.

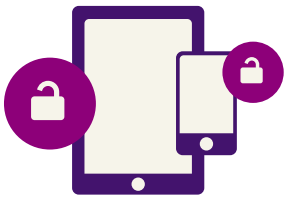
EN RÆKKE GODE RÅD, SOM ALLE I VIRKSOMHEDEN BØR FØLGE:

- Behandl virksomhedens data forsvarligt, og forhold dig kritisk til de netsteder, du besøger
- Pas på links i e-mails og fra sociale medier, som Facebook, Twitter og LinkedIn. Links på disse platforme bruges i stigende grad til at dirigere trafik videre til inficerede hjemmesider
- Husk at bruge gode og sikre kodeord – og udskift dem regelmæssigt. Et godt kodeord består af både bogstaver, tegn og tal. Man bør desuden undgå at genbruge sit password på flere forskellige platforme. Hvis det bliver knækket et sted – for eksempel på et Facebook-login, er det nemt for it-kriminelle at prøve på andre systemer – for eksempel en e-mail konto.

TIP TIL ET GODT PASSWORD

Brug f.eks. en sætning eller en sekvens af ord, som er lette at huske som: "Svend og Karen har 3 voksne børn". Passwordet bliver i dette tilfælde: "SoKh3vb"

- Lad være med at åbne og svare på e-mails med ukendt eller mistænkeligt indhold og afsender. Hverken banker eller SKAT beder om fortrolige oplysninger via e-mail
- Lad være med at installere ukendte programmer



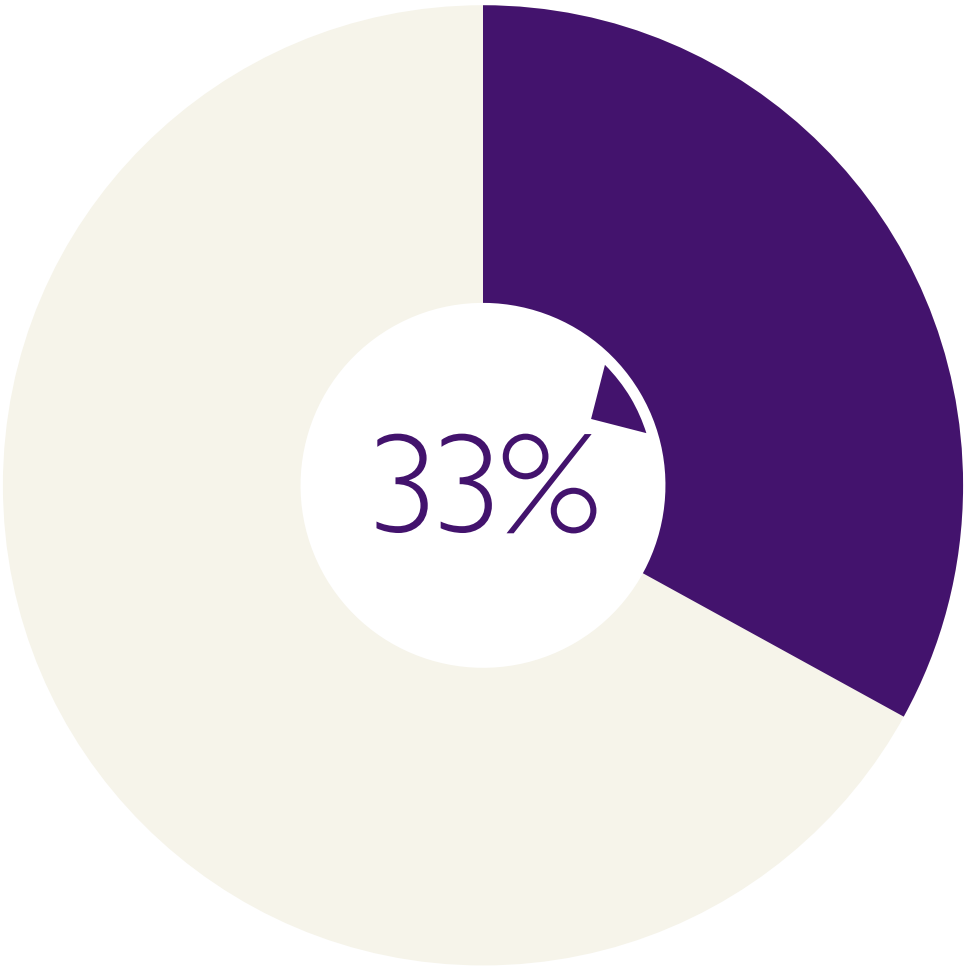
- Vær opmærksom på brugen af smartphones og tablets. De er ikke dækket af forsikringen i tilfælde af it-kriminalitet, men mange bruger enhederne til e-mails, sociale medier og netbank, der giver adgang til fortrolige oplysninger. Og får man eksempelvis stjålet en tablet eller smartphone, er det nemt for it-kriminelle at få adgang til data, der normalt er godt beskyttet på en pc, men ofte helt ubeskyttet på disse enheder.

Desuden er det en god idé, at I i ledelsen løbende holder øje med jeres netbankkonto. Gennemgå gerne kontoen 1-2 gange om ugen for uautoriserede bevægelser.

Banken dækker ikke

Rigtig mange tror, at banken dækker, hvis de får stjålet penge gennem virksomhedens netbank-konto. Virkeligheden er dog, at banken som udgangspunkt kun dækker tyveri fra privates netbankkonti – og altså ikke fra en virksomhedskonto. Som forening eller virksomhed hæfter I selv for hele det stjålne beløb.

Det er derfor en rigtig god idé at tjekke om jeres erhvervsforsikring dækker it-kriminalitet. En almindelig it-kriminalitetsdækning dækker netbanksindbrud og ofte også tab som følge af angreb af computervirus eller datasabotage.



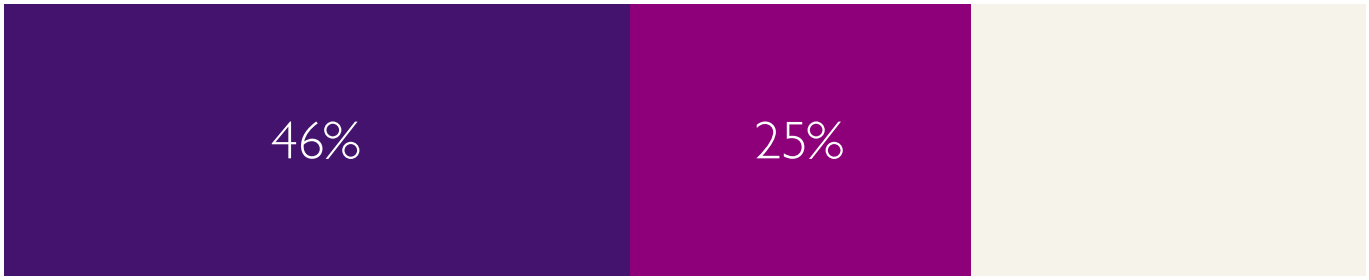
33 % tror, at banken dækker, hvis de får stjålet penge på virksomhedens netbank[8]

8. Undersøgelse blandt 232 mindre virksomheder (0-9 ansatte) udført af analyseinstituttet Wilke for Codan Forsikring, juli 2013

Hvis virksomheden rammes

Er uheldet ude og virksomheden rammes af et virusangreb, netbanksindbrud eller anden it-kriminalitet, skal I melde det til jeres forsikringsselskab. Man kan også anmelde angrebet til Politiet via Borger.dk eller Politiets hjemmeside.

Det er ikke lovpligtigt at melde it-kriminalitet til Politiet, men jeres informationer kan bidrage til at skabe mere viden om, hvordan angrebene sker, og på sigt hjælpe med at forebygge, at de sker igen.



46% af små danske virksomheder inden for brancherne service, detail og håndværk har ikke en forsikring mod it-kriminalitet. 25% ved ikke om de har det [9]

9. *Undersøgelse blandt 232 mindre virksomheder (0-9 ansatte) udført af analyseinstituttet Wilke for Codan Forsikring, juli 2013*

Codan Forsikring A/S

Gammel Kongevej 60
1790 København V

Tel 33 55 51 02

www.codan.dk