Deloitte.

Fem gode råd om forebyggelse af hackerangreb

Få styr på sikkerheden og sov roligt om natten

Vidste du, at …

… hackere især går efter de personfølsomme kundedata hos virksomheder? Kontaktoplysninger og kreditkortinformationer er i særlig høj kurs, da de kan bruges til yderligere berigelseskriminalitet i cyberspace.

… flere end hver tredje dansker kun i mindre grad har tillid eller slet ikke har tillid til, at private virksomheder håndterer personfølsomme data forsvarligt? Det er den mistillid den nye EU-forordning skal afhjælpe. Borgere skal føle sig trygge ved at udlevere deres personlige oplysninger, når de eksempelvis handler på nettet.

Data tages som gidsel

Trusselsbilledet ændrer sig konstant. Nye teknologier giver os nye forretningsmuligheder, men øger også antallet af indgange til virksomheders kritiske data. Risikoen for at data kommer i de forkerte hænder og tages som gidsel øges dagligt, fordi hackere anvender stadig mere avancerede metoder.

Der er ikke grund til, at du som virksomhedsejer bliver teknologiforskrækket over for teknologier som fx mobile, cloud og Internet of Things. Men der er grund til at undersøge, hvordan du beskytter din virksomheds kritiske data, og hvor modstandsdygtig din virksomhed er mod cyberangreb. Det gælder i særdeleshed for små og mellemstore virksomheder, som ikke har prioriteret datasikkerhed og derfor er nemme ofre.

Et selvstændigt marked

Cyberangreb er i dag et selvstændigt marked med sin egen værdikæde på The Dark Web. Nogle udvikler cyberangreb, andre sælger dem, og igen andre udfører dem. Hackerne konkurrerer om at levere de bedste cyber crime services, fordi der er gode penge at tjene på dine data.

Hackere tjener bl.a. penge på private virksomheder ved at:

- kryptere virksomheders kritiske data og afkræve dem penge, mod at virksomheder får nøglen til de krypterede data tilbage
- true med at give en kopi af virksomheders database til konkurrenter, medmindre man betaler en sum penge
- sælge persondata til andre, som udnytter disse i den videre fødekæde til bl.a. identitetstyveri
- overtage systemer for at fremprovokere dataoverførsler, eksempelvis pengetransaktioner

Hvorfor skal du interessere dig for cyberangreb?

- Fordi virksomheder gambler med cybersikkerheden trods massive advarsler fra myndighederne. Ifølge en rapport fra Danmarks Statistik fra december 2015 har over 60% af danske virksomheder ikke en politik for it-sikkerhed.
- Ifølge en undersøgelse gennemført af Opinion for Deloitte har over halvdelen af danske medarbejdere ikke viden om, hvordan de skal agere sikkert på internettet, mens de er på arbejde. Det indbefatter brug af passwords, opmærksomhed på mulig svindel, samt daglig omgang med følsomme data. Netop manglende viden om truslerne er den største risiko, og det er oftest medarbejdere, der er det svage led i sikkerhedskæden.
- Derudover træder den nye EU-persondataforordning snart i kraft. EU's eksisterende databeskyttelsesdirektiv fra 1995 er for længst blevet overhalet af nye teknologier, der sammenkobler data på kryds og tværs. Derfor indfører EU en forordning om beskyttelse af persondata, som træder i kraft i 2017 og vil medføre store stramninger og højere bøder fra dag ét.
- Persondataforordningen stiller især krav til dokumentation for, at data beskyttes, og at fx kunder får egenkontrol med data. Det betyder, at kunder skal have nem adgang til deres data hos jer, at de selv skal kunne flytte egne data til en anden serviceudbyder, at de skal underrettes om databrud inden for 24 timer, etc. Reglerne gælder for alle virksomheder i EU – og for virksomheder uden for EU, som handler med EU-lande. *Kilde: European Commission, Factsheet on data protection reform, 2012, "Why do we need an EU data protection reform?"*
- Endelig er der naturligvis de høje omkostninger ved at lade stå til. Nedetid, datatab, skade på virksomhedens omdømme, dalende kundetillid, usikkerhed blandt medarbejderne, tab af konkurrenceevne og genoprettelsesomkostninger kan bringe din virksomhed i knæ og er rigelig grund til, at du skal have styr på sikkerheden.

Hvad kan Deloitte gøre for dig?

Deloitte er kendt for at være en verdensomspændende revisionsvirksomhed. Halvdelen af organisationen yder dog uvildig rådgivning inden for andre områder end revision.

Cybersikkerhed er et voksende område i Deloitte, og vi har 50 personer i Danmark, der udelukkende beskæftiger sig med det

Deloitte har udviklet en Cyber Security KLAR-PARAT-START-pakke til små og mellemstore virksomheder, hvor du får:

- En årlig **vurdering** af din cybersikkerhed, herunder en it-risikoanalyse, der tager udgangspunkt i områder, hvor I er mest sårbare. Vurderingen viser, hvor udfordringerne er, og hvilke prioriterede initiativer skal igangsættes.
- Et årligt simuleret og **kontrolleret angreb** for at finde ud af, hvor modstandsdygtig I er over for tilfældige trusler fra internettet. Vi identificerer sårbarheder og anviser, hvordan sårbarhederne elimineres.
- En **projektplan**, der indeholder cyber security-aktiviteter, som er afstemt med jeres ressourcer og økonomi. Sparring og support i 12 måneder.

Deloitte er globalt førende

Deloitte er udnævnt som globalt førende inden for Cyber Security af Kennedy Consulting Research & Advisry. Ifølge deres seneste rapport har Deloitte de mest omfattende kompetencer på tværs af hele cyberspektret. Rapporten fremhæver desuden, at Deloitte hjælper virksomheder med at være på forkant, sætter barren for rådgivningsbehov inden for Cyber Security og beviser sit værd som forløber gennem sin dedikation til Cyber Security uden for kundepartnerskaber. Ved at samarbejde med universiteter om at forbedre pensum om emnet bidrager Deloitte til at opbygge en mere sikker fremtid for verden.

Fem gode råd

Sikkerhed er ikke en destination, men en rejse. Som virksomhedsejer kan du komme meget langt med nogle enkle gode råd.

1. **Afdæk sikkerhedsgraden i din virksomhed.** Har I implementeret sikkerhedspolitikker? Hvis ja, bliver de overholdt? Ved medarbejderne, hvad de skal holde øje med? Ved I, hvor I er mest sårbare?
2. **Risikovurdering og prioritering af indsatsområder**. Fokuser på det vigtigste først. Har I kritiske systemer, som er lette at få adgang til? Lever I op til den nye persondataforordning? Hvad er risikoen ved jeres sikkerhedsprioritering?
3. **Løs akutte problemer og test det reelle sikkerhedsniveau.** Løs akutte sikkerhedshuller og få indarbejdet en god it-sikkerhedsadfærd. Orienter medarbejdere om, hvad de skal være opmærksomme på. Dernæst skal I – gennem professionelle etiske hackere - teste, om medarbejderne ved, hvornår de hopper i fælden. Testen foretages et par gange om året og viser, hvor medarbejderne er usikre eller uopmærksomme på eventuelle trusler.
4. **Udarbejd en plan for forbedringer.** Efter testen kan I udarbejde en sikkerhedspolitik. Nu kender I de største trusler mod jeres virksomhed, og I ved, hvad I selv kan gøre for at eliminere dem. Uddeleger ansvaret for virksomhedens sikkerhed til en ressource og sørg for, at sikkerhedspolitikken er enkel. Fokuser på det vigtigste.
5. **Ingen panik.** Med ganske få håndtag kan I regulere og være på forkant med hackerne. Både du og dine medarbejdere kan sove trygt om natten, når I fokuserer de rigtige steder, dvs. der hvor det gør mest ondt i forretningen. Så gå ikke i panik. Gør it-sikkerheden håndterbar og lige til.