Masterclass Cybercrime

"Het overkomt mij toch niet!", is een veelvoorkomende uitspraak op de markt. Helaas is de realiteit dat het u wel kan overkomen! 98%[1] van alle bedrijven zijn het slachtoffer van een datahacking of poging daar toe. De Norton Symatec Security Survey toont aan dat:

- 29% op frequente basis onderhevig zijn aan een cyber aanval;
- 24% van de bedrijven schade en dataverlies oplopen;
- 20% van de aangevallen bedrijven hierna een inkomsten- of reputatieverlies ondervindt.

Bovendien is het voor hackers gemakkelijker om data van kleine en middelgrote organisaties te stelen, in vergelijking met bedrijven zoals: KPN of Philips:

- Kleinere organisaties hebben vaak een slechter veiligheidssysteem; wat hacken makkelijker maakt;
- Wanneer een kleinere organisatie bestolen of gehackt wordt, haalt dit niet vaak het nieuws, waardoor hackers rustig verder kunnen gaan zonder al te veel media aandacht.

Bijgaand voorbeelden van organisaties die slachtoffer zijn geworden van een hack.

1. Casus: Destination Hotels

Een hotelketen wordt gehackt en meer dan 700 creditcardgegevens vallen in verkeerde handen. Destination hotels, is het slachtoffer geworden van een enorme database hack die langer dan drie maanden heeft geduurd, waarbij er van meer dan 700 gasten creditcardgegevens zijn gestolen.

- Dit heeft geresulteerd in;
  - Een gemiddeld verlies van € 1.000 per credit card
  - Een totaalverlies van € 700.000 (€ 700 maal 1.000)
  - Reputatieschade van de hotelketen
  - Significant inkomstenverlies
  - Claims van de kaarthouders (aansprakelijkheid)
- Hoe heeft deze hack kunnen plaatsvinden?
  - Hoofdoorzaak; geen adequate beveiliging van de website

2. Casus: Elektrische huishoudelijke toestellen

Een hacker beweert 200.000 e-mailadressen en telefoonnummers van de website van een elektronica concern geplukt te hebben. Als gevolg hiervan kwam het bedrijf erachter dat de veiligheid van hun microsites (websites door hun gebruikt voor advertenties en andere acties) niet up to date was. De server van de websites was voor het laatst drie jaar geleden bijgewerkt, dat het succes van de hack verklaart. De hacker heeft een deel van de adressen en telefoonnummers uit de database online gezet en de rest van de gegevens verkocht aan spammers.

[1] Security Survey Symatec

Wat zullen de kosten omvatten?

– Forensisch onderzoek	€	89.000
– Juridische kosten	€	300.000
– Notificatie van de data inbreuk aan stakeholders	€	250.000
– Herstelkosten database	€	175.000
– Claims van consumenten	€	750.000
– Communicatiekosten	€	110.000

- Contactgegevens van de slachtoffers achterhalen;
- Het verzenden van een mailing;
- Een call center inschakelen om meteen vragen te kunnen beantwoorden;
- Media en PR campagne om de kosten en schade aan het merk te beperken.

Totaal kostenplaatje data inbreuk: € 1.674.000

3. Casus: Overslagbedrijf

Een overslagbedrijf gespecialiseerd in de opslag, ompakken, afzakken van koffie gaat een contract tekenen met een multinational. In het contract staat dat het overslagbedrijf gehouden is alle productiedetails geheim te houden en zich hiervoor te verzekeren. Enkele maanden later wordt het productiesysteem gehacked.

Wat zullen de kosten omvatten?

– Privacy/geheimhouding aansprakelijkheid (contractuele vergoeding)	€	50.000
– Kosten Inbreuk → forensisch ICT onderzoek	€	15.000
– Hacker schade → herstel netwerk + website + data	€	65.000

Totaal kostenplaatje data inbreuk: € 130.000

4. Casus: Advocaat

Een partner van een advocatenkantoor laat vier dossiers op de achterbank van de auto liggen. Na inbraak in de auto krijgt hij een telefoontje dat hij de dossiers kan terugkopen voor € 20.000.

De beroepsaansprakelijkheid zal pas gaan uitkeren wanneer de cliënten de advocaat aansprakelijk stellen, zover is het nu nog niet.

Het advocatenkantoor wil graag de afpersing laten analyseren, want hoe serieus is het dreigement? De Data Risks verzekering biedt een dekking voor de kosten als gevolg van afpersing. Met de Data Risks verzekering verzekert men data, zowel online als fysiek.