Cyberschades uit de praktijk

CHUBB®

CHUBB

Cybeschades uit de praktijk

Fout door werknemer	Impact	Kosten
Een recruiter van een zorginstelling stuurde per ongeluk het verkeerde bestand mee in een e-mail naar vier kandidaten. Het bestand bevatte namen, adressen en BSN-nummers van voormalige werknemers. De verzekerde belde het Chubb Cyber Incident Response nummer voor assistentie en een cyber incident manager werd aangesteld. Juridische adviseurs werden ingeschakeld om de met regelgeving samenhangende gevolgen te managen.	**Privacy-aansprakelijkheid** - onzorgvuldig beheer van persoonsgegevens en/of vertrouwelijke bedrijfsgegevens, inbreuk op het privacybeleid van de zorginstelling.	
	- Verweerkosten die voortvloeien uit de Meldplicht Datalekken	€ 65.000
	- Verweerkosten en schikkingsbedragen voor claims van werknemers van wie de identiteit openbaar is gemaakt	€ 115.000
	Cyber incidentkosten	
	- Kosten voor een cyber incident manager	€ 5.800
	- Melding aan getroffen personen	€ 3.500
	- Identiteitsdiefstal monitoringsdiensten voor getroffen personen	€ 15.000
	- Kosten voor juridisch advies	€ 12.000
Conclusie Het gaat bij cyber lang niet altijd om technologische incidenten. Veel schades die wij zien, zijn het gevolg van menselijke fouten.		**€ 216.300**

Distributed denial-of-service (DDoS) aanval	Impact	Kosten
Een distributed denial-of-service aanval vond plaats bij een datacentrum waar een website van een webshop werd gehost. De aanval overspoelde het netwerk van het datacentrum met zoveel verkeer dat het netwerk uitviel. Hierdoor was de webshop 6 uur ontoegankelijk voordat het back-up systeem de 100% functionaliteit hersteld had. In dit scenario was de online webshop de verzekerde. Nadat het Chubb Cyber Incident Response nummer was gebeld,werd een cyber incident manager aangesteld.	**Herstelkosten**	
	- Extra arbeidskosten om de website weer te laten functioneren	€ 10.000
	- Kosten van het inhuren van een externe serviceprovider	€ 14.000
	Bedrijfsschade	
	- Verlies van omzet en opbrengsten doordat de website niet functioneerde	€ 111.000
	Cyber incidentkosten	
	- Forensisch ICT-bedrijf	€ 14.000
	- Kosten voor juridisch advies	€ 11.500
	- Kosten voor cyber incident manager	€ 7.000
Conclusie Distributed denial-of-service (DDoS) aanvallen komen veelvuldiger voor doordat het gebruik van eenvoudig te hacken internet of things-apparatuur toeneemt. Om de impact van een scenario als dit zoveel mogelijk te beperken, is het belangrijk om een bedrijfscontinuïteitsplan op te stellen dat erop toeziet dat bedrijfskritische applicaties, systemen en activiteiten niet afhankelijk zijn van één kritieke ICT-leverancier. De cyber incident managers en leveranciers van Chubb zijn ervaren in het omgaan met DDoS-aanvallen en helpen om uw bedrijf zo snel mogelijk weer operationeel te krijgen.		**€ 167.500**

Aanval door ransomware	Impact	Kosten
Een werknemer van een productiebedrijf van auto-onderdelen klikte op een link in een e-mail waardoor malware op de server van het bedrijf werd gedownload en alle gegevens werden versleuteld. Op de computer van de werknemer verscheen een e-mail waarin € 10.000 in Bitcoin werd geëist binnen 48 uur in ruil voor de decryptie-sleutel. Het bedrijf belde het Chubb Cyber Incident Response nummer voor hulp. De toegewezen cyber incident manager regelde forensische ICT-experts om de echtheid van de bedreiging te beoordelen en te bepalen of het bedrijf de betaling van het losgeld kon voorkomen.	**Aansprakelijkheid voor netwerkbeveiliging** - het falen van de netwerkbeveiliging van verzekerde om kwaadwillige handelingen via de computer te voorkomen	Zie cyber incidentkosten (onder)
	Digitale afpersing - kosten voor de aanpak van afpersingsbedreigingen om informatie of een kwaadaardige code vrij te geven, tenzij afpersingsgeld wordt betaald	
	- Kosten voor een ICT-consultant om o.a. de back-up- mogelijkheden te beoordelen	€ 16.000
	Cyber incidentkosten	
	- Forensische onderzoekskosten om de malware op te sporen, de impact te analyseren en de schade in kaart te brengen	€ 21.000
	- Kosten voor juridisch advies	€ 8.000
	- Kosten voor cyber incident manager	€ 7.000
	Verlies van data - kosten voor het vervangen van verloren of beschadigde data	€ 17.000
Conclusie Hoewel de eis in Bitcoin lager was dan de kosten die onder de verzekering waren gemaakt, wordt door zowel Europol als de FBI aangeraden om geen cyber losgeld te betalen. Niet alleen worden door het betalen van het losgeld criminele activiteiten in stand gehouden, maar het impliceert ook een gebrek aan effectieve en betrouwbare back-up procedures van een bedrijf. Back-ups moeten off-site en buiten het netwerk om worden opgeslagen. Desondanks begrijpt Chubb dat het betalen van losgeld onder sommige omstandigheden de beste optie kan zijn.		**€ 69.000**

Media - per e-mail in diskrediet brengen	Impact	Kosten
Een werknemer van een consultancybedrijf stuurde een interne e-mail met negatieve opmerkingen over een dienstverlener. De e-mail werd naar anderen binnen de organisatie verspreid en uiteindelijk ook extern doorgestuurd. De dienstverlener zag de e-mail en begon een rechtszaak wegens laster tegen het adviesbureau vanwege de nadelige gevolgen ten aanzien van zijn reputatie.	**Media-aansprakelijkheid** - aanspraken van derden door uitingen van verzekerde op internet. Onrechtmatige daden omvatten o.a. smaad, laster ten aanzien van personen en plagiaat.	
	- Verweerkosten en schikkingsbedragen voor claims van de serviceprovider	€ 175.000
	Cyber incidentkosten	
	- Crisis communicatiediensten	€ 14.000
	- Kosten voor een pr-deskundige om reputatieschade te beperken	€ 18.000
	- Kosten voor een cyber incident manager	€ 3.500
Conclusie Vanwege de gevoeligheid van een dergelijke claim en de potentiële reputatieschade is het voor bedrijven belangrijk om snel te handelen en eventuele schade te beperken. Door het Chubb Cyber Incident Response nummer te bellen, kunnen we zorgen dat de juiste specialisten worden aangesteld om de klant te ondersteunen en effectief met de serviceprovider te communiceren om de schade te beperken en de zaak zo goed mogelijk af te handelen.		**€ 210.500**

Onbevoegde toegang	Impact	Kosten
Hackers verschaften zich toegang tot gegevens op het netwerk van een groep scholen via een lek in het netwerk. De gegevens bevatten namen, e-mailadressen, ISDN-nummers en financiële gegevens van oud- en huidige docenten en studenten. Nadat meerdere docenten en leerlingen verdachte activiteiten op hun e-mail meldden, ontdekte de ICT-afdeling dat er een onbevoegde gebruiker op het systeem zat. De school belde het Chubb Cyber Incident Response nummer en een cyber incident manager werd toegewezen.	**Privacy-aansprakelijkheid** - onzorgvuldig beheer van persoonsgegevens en/of vertrouwelijke bedrijfsgegevens	
	- Verweerkosten naar aanleiding van regelgeving zoals de Meldplicht Datalekken	€ 87.000
	- Verweerkosten en schikkingsbedragen voor claims van personen van wie de identiteit is gestolen	€ 46.000
	Aansprakelijkheid voor netwerkbeveiliging - het falen van verzekerde om het netwerk effectief te beschermen tegen malware, hacking, denial-of-service aanvallen of ongeoorloofd gebruik of toegang	
	Cyber incidentkosten	
	- Kosten van forensisch onderzoek om het lek te lokaliseren, de impact te analyseren en de omvang van het verlies in kaart te brengen	€ 93.500
	- Melding aan de getroffen personen	€ 1.100
	- Identiteitsdiefstal monitoringdiensten voor de getroffen personen	€ 7.000
	- Kosten voor het opzetten van een callcenter voor vragen	€ 10.500
	- Kosten voor een pr-deskundige om de reputatieschade te beperken	€ 15.000
	- Kosten voor juridisch advies	€ 11.500
	- Kosten voor een cyber incident manager	€ 10.500
Conclusie Dit scenario toont aan hoe belangrijk het is uw informatie afdoende te beveiligen. Up-to-date firewalls, inbraakdetectiesoftware en versleuteling van databases zijn slechts een paar manieren om op verantwoorde wijze de privacy van de gegevens van de werknemer en klant te beschermen. Dit voorbeeld wijst ook op de vele manieren waarop de Chubb verzekering op cyberincidenten kan reageren. De cyber incident manager helpt bij het organiseren van de bijna tien verschillende diensten in verband met deze gebeurtenis, van verweerkosten tot pr-kosten en nog veel meer.		**€ 282.100**

Fraude bij betalingsverkeer	Impact	Kosten
Een werknemer kreeg een telefoontje 'van de bank van het bedrijf' waarin werd gezegd dat er een probleem met een betaling was, mogelijk veroorzaakt door een virus. De beller vertelde de werknemer dat de betaling handmatig zou moeten worden gedaan en slaagde erin een aantal beveiligingscodes te achterhalen. De werknemer vond het verdacht en waarschuwde zijn manager die onmiddellijk de bank op de hoogte bracht. Toen de bank de rekening blokkeerde waren er helaas al acht transacties voor in totaal € 500.000 verricht.	**Fraude schade** - het frauduleus verkrijgen of toe-eigenen van geld, waardepapieren of zaken	€ 500.000
Conclusie Dergelijk fraudes, ook wel social engineering genoemd, dat in frauduleuze betalingen resulteert, wordt doorgaans beter afgedekt door een fraudeverzekering. Een cyberverzekering kan hier mogelijk deels dekking voor bieden. In sommige scenario's kan social engineering tot verlies van gevoelige gegevens of persoonsgegevens leiden, dat onder een cyberpolis gedekt kan zijn. Het vanaf het begin identificeren van social engineering-methoden kan helpen om in beide scenario's de schade te beperken.		**€ 500.000**

Fraude bij betalingsverkeer	Impact	Kosten
Het netwerk van een middelgroot advocatenkantoor werd gehackt. Gevoelige klantinformatie was mogelijk in gevaar, waaronder: een overnamekandidaat van een beursgenoteerde onderneming, een beoogd technologiepatent van een andere beursgenoteerde onderneming, een voorlopige prospectus van een participatiemaatschappij en een aantal lijsten met persoonsgegevens van eisers in een collectieve rechtszaak. Het bedrijf kreeg toen een telefoontje waarin geëist werd om € 30.000 te betalen om de informatie niet op de zwarte markt te verkopen. Het advocatenkantoor nam contact op met het Chubb Cyber Incident Response nummer, een cyber incident manager werd toegewezen en forensische ICT-experts en een juridisch adviseur werden ingeschakeld om het incident aan te pakken.	**Privacy-aansprakelijkheid** - onzorgvuldig beheer van persoonsgegevens en/of vertrouwelijke bedrijfsgegevens **Aansprakelijkheid voor netwerkbeveiliging** - wegens het onvoldoende beveiligen van het netwerk om effectief te beschermen tegen malware, hacking, denial-of-service aanvallen of ongeoorloofd gebruik of toegang - Verweerkosten en schikkingsbedragen van collectieve rechtzaken **Cyber incidentkosten** - Forensische onderzoekskosten om het lek in het netwerk op te sporen, de impact te analyseren en de schade in kaart te brengen - De kosten voor het opzetten en onderhouden van een callcenter voor vragen - Kosten voor een pr-deskundige om de reputatieschade te beperken - Kosten voor juridisch advies - Kosten voor een cyber incident manager **Digitale afpersing** - kosten in verband met de aanpak van afpersingsbedreigingen om informatie of een code vrij te geven, tenzij afpersingsgeld wordt betaald - Kosten voor een crisisonderhandelaar - Kosten voor juridisch advies - Kosten voor een ICT-consultant	 € 116.000 € 51.000 € 9.350 € 14.000 € 32.700 € 9.300 € 4.500 € 2.300 € 25.700
Conclusie Hoewel losgeld betalen voor bedrijven soms de beste oplossing lijkt, is het dit vaak niet. Door het Chubb Cyber Incident Response nummer te bellen, kan de cyber incident response manager de klant vanaf het begin adviseren welke stappen moeten worden genomen. We hebben gevallen gezien waarin het losgeld werd betaald en de informatie alsnog online werd gepubliceerd. Er bestaat een risico dat als het losgeld niet wordt betaald, de informatie wordt gedeeld, maar de cyber incident manager zal ervoor zorgen dat de juiste deskundigen worden benoemd om met deze situatie om te gaan.		**€ 264.850**

Contact

Chubb European Group Limited
Marten Meesweg 8-10
3068 AV Rotterdam
T. 0800 22 55 223 (Nederland)
T. +31(0)10 289 35 00

E. info.benelux@chubb.com
www.chubb.com/nl

Chubb. Insured.℠

04/17 NT-3986L