Schadevoorbeelden Cyber

CHUBB®

CHUBB

Schadevoorbeelden Cyber

Scenario 1: Fout door werknemer	Impact	
Een recruiter van een zorginstelling stuurde per ongeluk het verkeerde bestand mee in een e-mail naar vier kandidaten. Het bestand bevatte demografische informatie met de namen, adressen en BSN-nummers van 43.000 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 regelgevingsgevolgen te managen.	**Privacy-aansprakelijkheid** - wanbeheer van persoonsgegevens en/of vertrouwelijke bedrijfsgegevens, inbreuk op het privacybeleid van het bedrijf.	
	- Verweerkosten die voortvloeien uit een regelgevingsprocedure	€65.000
	- Verweerkosten en schikkingsbedragen voor claims van werknemers van wie de identiteit is gestolen	€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 Ze lijken onschuldig, maar menselijke fouten kunnen heel kostbaar zijn, en ze komen vaker voor dan verwacht. Het is belangrijk om te realiseren dat het bij cyber niet alleen om technologische incidenten gaat. Veel schades die wij zien zijn het gevolg van menselijke fouten.		**Totale kosten €216.300**

Scenario 2: Distributed denial-of-service (DDoS) aanval	Impact	
Een distributed denial-of-service aanval vond plaats op een datacentrum waar een website van een webshop was gehost. De aanval, die gebruik maakte van gehackte internet of things-apparatuur, overspoelde het netwerk van het datacentrum met zoveel verkeer dat het netwerk uitviel. Hierdoor was de website van de webshop 6 uur ontoegankelijk voordat het back-up systeem in staat was om de 100% functionaliteit te herstellen. In dit scenario was de verzekerde een online retailer. 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 om een externe serviceprovider in te huren	€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 worden steeds krachtiger doordat het gebruik van eenvoudig gehackte 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 ervoor zorgt 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.		**Totale kosten €167.500**

Scenario 3: Anvallen door ransomware	Impact	
Een werknemer van een productiebedrijf van auto-onderdelen klikte op een kwaadaardige 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 die eiste dat binnen 48 uur €10.000 in Bitcoin werd betaald 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 validiteit 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 in verband met de aanpak van afpersingsbedreigingen om informatie of een kwaadaardige code vrij te geven, tenzij afpersingsgeld wordt betaald	
	- Kosten voor een ICT-consultant om de back-upmogelijkheden te beoordelen	€16.000
	Cyber incidentkosten	
	- Forensische onderzoekskosten om de malware op te sporen, de impact te analyseren, te zorgen voor insluiting en de schade te berekenen	€21.000
	- Kosten voor juridisch advies	€8.000
	- Kosten voor cyber incident manager	€7.000
	Verlies van datagegevens - kosten in verband met het vervangen van verloren of beschadigde gegevens	€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. Chubb begrijpt dat in bepaalde omstandigheden het betalen van losgeld de laatste maar beste optie is. Om die reden zijn Chubb cyber incident leveranciers uitgerust met een Bitcoin-portemonnee indien nodig.		**Totale kosten €69.000**

Scenario 4: Media - per e-mail in diskrediet brengen	Impact	
Een werknemer van een consultancybedrijf stuurde een interne e-mail met negatieve opmerkingen over een serviceprovider. De e-mail werd binnen de organisatie naar anderen verspreid en uiteindelijk ook extern doorgestuurd. De serviceprovider zag de e-mail en begon een rechtszaak wegens laster tegen het adviesbureau vanwege de nadelige gevolgen voor de reputatie van de serviceprovider.	**Media-aansprakelijkheid** - aanspraken van derden die voortvloeien uit media-activiteiten van verzekerde via internet. Onrechtmatige daden omvatten smaad, laster ten aanzien van personen en het in diskrediet brengen van producten, plagiaat en nog veel meer	
	- 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 van een klant, is het voor bedrijven belangrijk om snel te handelen om eventuele schade te beperken. Door het Chubb Cyber Incident Response nummer te bellen, kunnen we zorgen dat de juiste specialisten worden aangesteld om met de klant te werken en effectief met de serviceprovider te communiceren om problemen op te lossen en de zaak af te handelen.		**Totale kosten €210.500**

Scenario 5: onbevoegde toegang	Impact	
Hackers kregen ongeoorloofd toegang tot gegevens op het netwerk van een groep scholen als gevolg van een onbekende kwetsbaarheid van het netwerk. De informatie bevatte 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 er werd een cyber incident manager toegewezen.	**Privacy-aansprakelijkheid** - wanbeheer van persoonsgegevens en/of vertrouwelijke bedrijfsgegevens - Verweerkosten die voortvloeien uit een regelgevingsprocedure als gevolg van onverantwoordelijk beheer van privé-informatie - Verweerkosten en schikkingsbedragen voor claims van een individu van wie de identiteit is gestolen **Aansprakelijkheid voor netwerkbeveiliging** - het falen om het netwerk van verzekerde effectief te beschermen tegen malware, hacking, denial-of-service aanvallen of ongeoorloofd gebruik of toegang **Cyber incidentkosten** - Forensisch onderzoek naar de kosten om de kwetsbaarheid te lokaliseren, impact te analyseren, zorgen voor insluiting en het berekenen van de omvang van het verlies - Melding aan de getroffen personen - Identiteitsdiefstal monitoringdiensten voor de getroffen personen - Kosten voor het opzetten en exploiteren van een callcenter voor vragen - Kosten voor een pr-deskundige om de impact op de reputatieschade te beperken - Kosten voor juridisch advies - Kosten voor een cyber incident manager	€87.000 €46.000 €93.500 €1.100 €7.000 €10.500 €15.000 €11.500 €10.500
Conclusie Dit scenario wijst op het belang van noodzakelijke beveiligingen voor het opslaan van gevoelige informatie. 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.		**Totale kosten €282.100**

Scenario 6: Fraude bij betalingsverkeer	Impact	
Een werknemer kreeg een telefoontje ogenschijnlijk afkomstig 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 om een aantal bankbeveiligingscodes te achterhalen. De werknemer vond het verdacht en waarschuwde zijn manager die onmiddellijk de bank op de hoogte bracht. De bank blokkeerde de rekening, maar toen waren 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 Social engineering dat in frauduleuze betalingen resulteert wordt beter afgedekt door een fraudeverzekering dan door een cyberverzekering. 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.		**Totale kosten: €500.000**

Scenario 7: Hack - Resulterend in afpersing	Impact	
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** - wanbeheer van persoonsgegevens en/of vertrouwelijke bedrijfsgegevens **Aansprakelijkheid voor netwerkbeveiliging** - aansprakelijkheid die voortvloeit uit het falen om het netwerk van verzekerde effectief te beschermen tegen malware, hacking, denial-of-service aanvallen of ongeoorloofd gebruik of toegang - Verweerkosten en schikkingsbedragen van collectieve rechtszaken **Cyber incidentkosten** - Forensische onderzoekskosten om de kwetsbaarheid van het netwerk op te sporen, de impact te analyseren, te zorgen voor insluiting en de schade te berekenen - De kosten voor het opzetten en onderhouden van een callcenter voor vragen - Kosten voor een pr-deskundige om de impact op 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 kwaadaardige code vrij te geven, tenzij afpersingsgeld wordt betaald - Kosten voor een crisisonderhandelaar - Kosten voor juridisch advies - Kosten voor een ICT-consultant - Betaling afpersing	€116.000 €51.000 €9.350 €14.000 €32.700 €9.300 €4.500 €2.300 €25.700 €30.000
Conclusie Cyber losgeld kan beter niet betaald worden, maar veel klanten zijn zich daar niet van bewust . 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.		**Totale kosten €294.850**

Chubb. Insured.℠

04/17 NT-3986L