WHITEPAPER

CYBERCRIME

024 324 76 00 info@ghw.nl www.ghw.nl

ghw
VERZEKERT PERSOONLIJK

CYBERCRIME

Cybercrime is één van de snelst groeiende vormen van misdaad van de laatste jaren. Omdat ons leven zich steeds meer digitaal afspeelt, neemt ook de kans op online criminaliteit toe. Verlies van data en hacking zijn hierbij een paar voorbeelden. Schade van dit soort incidenten is vaak niet gedekt onder een computer- en/of andere schadeverzekering.

Cybercrime is een vorm van criminaliteit waarbij internet-criminelen inbreken op bijvoorbeeld een computer, telefoon of het complete netwerk van jouw organisatie. ICT is bij deze vorm van criminaliteit zowel het doel als het middel.
Het risico op cybercrime wordt helaas nog onderschat.
Dat overkomt mij toch niet? Maar iedereen is een potentieel doelwit. Of het nu gaat om een menselijke fout of een aanval van buitenaf, de gevolgen zijn niet te overzien.
Een virus ken je waarschijnlijk wel, maar cybercrime gaat veel verder dan dat.

INHOUD

024 324 76 00 info@ghw.nl www.ghw.nl

ghw
VERZEKERT PERSOONLIJK

1 Vormen van cybercrime

De digitale veiligheid staat aan vele dreigingen bloot. De meest voorkomende vormen zijn:

Verlies persoonsgegevens

Sinds 1 januari 2016 is het wettelijk verplicht om datalekken te melden. Zowel grootschalige inbraak als iedere vorm van data verlies, diefstal of onbevoegd gebruik van persoons-gegevens wordt gezien als een datalek. Wie data laat lekken of persoonsgegevens verwerkt zonder zich aan de wet te houden, loopt kans op hoge boetes.

Phishing

Phishing is een vorm van cybercrime die we steeds vaker zien: via een valse e-mail of website wordt gevraagd naar je persoonlijke gegevens. Internetcriminelen kunnen dit ook vanuit jouw bedrijfsnaam doen. Geef nooit zomaar wachtwoorden, pincodes of andere persoonlijke gegevens door n.a.v. dit soort berichten.

Malware

Malware is een verzamelnaam voor schadelijke software. Door de computer te besmetten met malware kunnen criminelen toegang krijgen tot de computer en je bestanden vergrendelen. Een bekend voorbeeld van malware is het virus. Een virus is een computerprogramma dat zich in een bestand op je computer nestelt. Er kan informatie op je computer verspreid worden, maar het is ook mogelijk dat je computer hierdoor niet meer te gebruiken is.

DdoS aanvallen

Bij een DdoS aanval wordt de server overbelast met als doel de website of internetdienst (tijdelijk) onbruikbaar te maken.

Hacking

Zonder toestemming binnendringen van een computernetwerk door de beveiliging te doorbreken.

Cyberafpersing

Het van buitenaf binnendringen van een computernetwerk. Zodra hackers toegang hebben tot het digitale netwerk starten zij met het afpersen van de organisatie of een persoon. Je krijgt pas weer toegang tot de computer(s) of telefoon(s) zodra er geld betaald is.

2 Belang cybersecurity

Steeds meer gevoelige gegevens worden gedeeld via het internet en online opgeslagen. Veilige en betrouwbare ICT is van groot belang voor onze samenleving en economie. Een samenleving zonder internet is eigenlijk niet meer denkbaar. Deze toenemende afhankelijkheid maakt onze samenleving kwetsbaarder voor misbruik en uitval. Digitale veiligheid, ofwel cybersecurity, is dan ook van essentieel belang.

Cybersecurity is een gezamenlijke verantwoordelijkheid van overheid, bedrijfsleven en burgers. Al deze partijen zijn zelf verantwoordelijkheid om hun eigen kwetsbaarheid te verminderen.
Een intensieve samenwerking is van groot belang, want de kennis is verspreid over vele verschillende partijen.

Deze toenemende afhankelijkheid van ICT maakt onze samenleving kwetsbaarder voor misbruik en uitval.

Wetgeving

In de afgelopen jaren is de wet ingrijpend aangescherpt. Dit moet de aanpak van internet criminaliteit vereenvoudigen.

- Politie en het openbaar ministerie krijgen voortaan de mogelijkheid op afstand onderzoek te doen in computers van criminelen. Digitale communicatie mag worden afgetapt.
- Mogelijke verdachten mogen worden verplicht mee te werken aan het ontsleutelen van bestanden op hun computer.
- Het (door)verkopen van informatie en dit online publiceren wordt strafbaar.
- Malafide webshops die goederen of diensten te koop aanbieden, maar niets leveren kunnen strafrechtelijk worden aangepakt.

3 De cyberverzekering

Wat veel mensen niet weten is dat schade als gevolg van een cyberincident vaak niet gedekt is onder een computer- en/of andere schadeverzekering. Daarnaast stelt ook de Wet Meldplicht Datalekken strenge eisen aan het veilig bewaren van gegevens (van derden). Dit vergroot het aansprakelijkheidsrisico.

De oplossing zit dan ook in een specifieke verzekering, te weten de cyberverzekering. Wat er precies wel en niet onder jouw cyber-verzekering valt, verschilt per verzekeraar. Cyberverzekeringen dekken veelal de volgende risico's:

Systeeminbraak

(hieronder vallen kosten als gevolg van inbraak op systemen of data)

- Kosten van (digitaal) forensisch onderzoek door externe deskundigen naar de oorzaak van hacking of verlies van data.
- Kosten die nodig zijn om de identiteit van betrokkenen te achterhalen.
- Kosten van communicatie met klanten, toezichthouders, justitie, creditcard-maatschappijen en andere belang-hebbenden.
- Kosten voor extra klantenondersteuning, crisismanagement en herstel van jouw reputatie.
- Civielrechtelijke boetes opgelegd door toezichthouders of andere verplichte vergoedingen.

Privacy

(hieronder vallen kosten als gevolg van gestolen privacy gevoelige gegevens)

- Kosten van onderzoek door bijvoorbeeld justitie of creditcardmaatschappijen.
- Claims van individuele personen, boetes opgelegd door toezichthouders of andere verplichte vergoedingen.

Hacking

- Reparatie, vervanging of herstel van websites, programma's, netwerk, computer-systeem, softwareprogramma's of data.
- Kosten van gestolen software of data.
- Kosten van onderzoek en advies in systeembeveiliging.

Cyberafpersing

- Het beschadigen of vernietigen van jouw website, intranet, netwerk, computer-systeem, programma's of elektronische data.
- Het openbaar maken of misbruiken van vertrouwelijke informatie die je in elektronische vorm houdt.

Bedrijfsschade

- Schade als de bedrijfsactiviteiten stil komen te liggen door een cyberaanval.

4 Kosten

Een cyberverzekering beschermt jouw organisatie tegen de gevolgen van cyber- en data risico's.

De kosten van jouw cyberverzekering zijn afhankelijk van een aantal factoren:

- Soort bedrijf
- Het verzekerd bedrag
- De omzet
- Eventuele dekkingsuitbreidingen

Met een cyberverzekering worden schades niet alleen financieel afgehandeld, maar je krijgt ook hulp en bijstand op het gebied van cyber-incidenten.
Voor ieder bedrijf dat beschikt over vertrouwelijke informatie en/of klantgegevens heeft een cyberverzekering dan ook zin.
Iedere verzekeraar heeft zijn eigen dekkingsgebieden, beperkingen en uitsluitingen. Het is goed om te kijken wat je precies nodig heeft. GHW adviseert jou graag.

Neem daarvoor contact met ons op.

Met een cyberverzekering worden schades niet alleen financieel afgehandeld, maar je krijgt ook hulp en bijstand op het gebied van cyberincidenten.

024 324 76 00 info@ghw.nl www.ghw.nl

ghw VERZEKERT PERSOONLIJK

5 Schadevoorbeelden Chubb

Scenario 1: Fout door werknemer

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.

Impact	**Kosten**
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
	Totale kosten **€ 216.300**

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.

024 324 76 00 info@ghw.nl www.ghw.nl

Scenario 2: Aanvallen door ransomware

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.

Impact	Kosten
Aansprakelijkheid voor netwerkbeveiliging Het falen van de netwerkbeveiliging van verzekerde om kwaadwillige handelingen via de computer te voorkomen.	
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- up mogelijkheden 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
	Totale kosten **€ 69.000**

Conclusie
Hoewel de eis in Bitcoin lager was dan de kosten die onder de verzekering waren gemaakt, wordt door zowel de politie en andere wetgevende instanties 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.

Wil je persoonlijk advies over onze cyberverzekering?

Neem dan contact met ons op. Nadat we jou hebben leren kennen zullen wij je adviseren over de financiële producten die het beste bij jou passen.
GHW verzekert persoonlijk en daar zijn we heel eerlijk in.

Bezoekadres
Takenhofplein 3, 6538 SZ Nijmegen

Postadres
Postbus 1061, 6501 BB Nijmegen

info@ghw.nl
www.ghw.nl
024 324 76 00

Volg ons op Social media:

ghw
VERZEKERT PERSOONLIJK