Techniek Nederland Verzekeringen

Cyberrisico's in de installatie- en technische detailhandelsbranche

“Cybercrime kost Nederland alleen al 10 miljard euro per jaar”

Meest voorkomende vormen

Er is sprake van cybercrime als kwaadwillende een bedrijf of persoon bewust saboteren. Echter, ontstaan er ook veel incidenten door eigen fout.

- *Verlies persoonsgegevens:* Sinds 1 januari 2016 is het wettelijk verplicht om datalekken te melden. Zowel grootschalige inbraak als iedere vorm van data kwijtraken, diefstal of onbevoegd gebruik van persoonsgegevens telt als een datalek. Denk hierbij aan foutief verstuurde e-mails met persoonsinformatie, niet goed afgeschermde delen van websites, zoekraken van USB-sticks, telefoon, laptops etc. Wie data laat lekken of persoonsgegevens verwerkt zonder zich aan de wet te houden, loopt kans op hoge boetes. Het maakt daarbij niet uit of er sprake is van cybercrime.
- *Phishing:* Het oplichten van mensen door ze te lokken naar een valse (bank)website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam, wachtwoord of creditcardnummer.

- *Malware en virussen:* Iedere vorm van software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot computersystemen.
- *DDOS-aanvallen:* Pogingen om een computernetwerk of dienst onbruikbaar te maken. Meestal worden hiervoor computers van anderen gehackt, die zich daar zelf niet van bewust zijn.
- *Hacking:* Het door onbevoegde derden zonder toestemming binnendringen van een computernetwerk door de beveiliging te doorbreken.
- *Spam:* Het ongewenst ontvangen van e-mails of ongewenste (vaak commerciële) informatie in nieuwsgroepen.
- *Afpersing:* Het van buitenaf binnendringen van een kantoornetwerk met als doel financieel nadeel toe te brengen. Dat kan door een virus te verspreiden, waardoor het netwerk van het kantoor geheel wordt geblokkeerd. Het kantoor ontvangt vervolgens een ‘ransom-mail’ met de mededeling dat het netwerk weer zal worden vrijgegeven na voldoening van een in het mailbericht genoemd bedrag.
- *Cryptohacking:* Het digitaal stelen van cryptomunten zoals bitcoins.
- *Botnets:* Het van buitenaf misbruiken van uw computer voor criminele activiteiten zonder dat u dit merkt.

Zichtbare en onzichtbare kosten

Veel bedrijven hebben geen volledig beeld van de kosten die gepaard gaan met cyberincidenten.

Denk hierbij onder andere aan:

- Systeemherstel.
- Kosten die gemaakt moeten worden voor het melden van een lek bij de betreffende toezichthouder.
- Bestuurlijke boetes bij een datalek.
- PR/crisiscommunicatie.
- Advocaat- en proceskosten.
- Forensisch onderzoek.
- Melding maken aan uw klanten.
- Niet kunnen doorwerken tijdens een incident (verstoring bedrijfscontinuïteit).
- Waardedaling van de handelsnaam (reputatieschade).
- Verlies van intellectueel eigendomsrechten of bedrijfsgeheimen.
- Klanten die geen orders kunnen plaatsen en naar een concurrent gaan.

Preventie tips

Het voorkomen van cybercrime vergt continue aandacht. Criminelen worden steeds professioneler. Medewerkers dienen voortdurend geïnstrueerd te worden en software en antivirussoftware vergen steeds nieuwe updates.

- Neem privacy- en gegevensbescherming integraal op in uw bedrijfscultuur.
- Belast één persoon met de eindverantwoordelijkheid voor beveiliging en gegevensbescherming.
- Implementeer een programma voor continue opleiding en bewustmaking van uw medewerkers.
- Zorg voor waterdichte contracten met leveranciers en relaties.
- Identificeer en classificeer de door de organisatie verzamelde en opgeslagen informatietypen/-soorten.
- Beperk het aantal verzamelde, bewaarde persoonsgegevens en vertrouwelijke informatie tot het strikt noodzakelijke minimum.

“Ruim 60 procent van ondernemend Nederland heeft inmiddels te maken gehad met cybercrime en het aantal aanvallen neemt nog steeds sterk toe.”

- Evalueer en actualiseer regelmatig de bestaande veiligheidsmaatregelen, plannen en procedures.
- Voer continu risicobeoordelingen uit en ga na hoe de vastgestelde risico’s kunnen worden vermeden of beperkt:
  - Tref administratieve voorzorgsmaatregelen.
  - Tref fysieke voorzorgsmaatregelen.
  - Tref technische voorzorgsmaatregelen.
- Bereid u voor op incidenten. Maak een incident responseplan.

Preventie heeft niet alleen te maken met softwarematige beveiligingen. Uiteraard zijn een gedegen, up-to-date firewall, antivirusprogramma en recente softwareversie van belang. Maar minstens zo belangrijk zijn preventieve maatregelen zoals:

- geen links of bijlagen aanklikken in e-mails, op internetsites e.d.;
- verdachte mails direct deleten (ook uit de ‘deleted files’ van uw mailprogramma);
- geen onbekende USB-sticks gebruiken;
- alleen sites bezoeken waarvan u zeker weet dat ze veilig zijn;
- alleen bestanden downloaden waarvan u zeker weet dat ze veilig zijn;
- sterke wachtwoorden gebruiken en regelmatig wijzigen (maak gebruik van een wachtwoord opslagprogramma);
- zorg voor een gedegen back-up systeem waarbij de back-ups niet online of via uw computer bereikbaar zijn.

Cyberverzekering

Hoewel veel mensen dit niet weten, is schade als gevolg van een cyberincident vaak niet gedekt onder een normale computerverzekering. Het is echter wel verzekerbaar.

Dekking

De volgende kosten zijn onder de meeste cyberverzekeringen gedekt:

- Aansprakelijkheid: Schadevergoeding en juridische bijstand in geval van aanspraken van derden als gevolg van verlies van persoonsgegevens en/of bedrijfsinformatie.
- Boetes (mits wettelijke toegestaan): Kosten voor onderzoek door een toezichthouder, juridische bijstand, bestuurlijke boetes.
- Digitale media: Schadevergoeding en kosten van verweer in verband met aanspraken van derden tegen u die voortvloeien uit uw multimedia-activiteiten. Bijvoorbeeld smaad en laster of plagiaat.
- Cyber-/privacy-afpersing, waaronder ransomware.
- Hacking telefooncentrale: Vergoeding van de belkosten.
- Netwerkonderbreking: Gederfde nettowinst in verband met netwerkonderbreking.
- Incident response: Kosten (forensisch)onderzoek, PR, klant notificatiekosten, kredietbewaking, IT-diensten.

Incident response

Gekoppeld aan de cyberverzekeringen van Techniek Nederland is een incident response. Dat is een alarmteam bestaande uit computerspecialisten en advocaten die u bijstaan in het geval er toch iets mocht gebeuren. Dit team is 24/7 bereikbaar en zorgt ervoor dat u zo snel mogelijk weer aan de slag kunt, met zo min mogelijk technische, juridische en administratieve problemen.

U hoeft alleen het alarmnummer te bellen dat u van ons heeft ontvangen. Het incident response team onderneemt aan de hand van het probleem actie.

Dat kan juridisch bijvoorbeeld zijn:

- advisering over eventuele melding bij de Autoriteit Persoonsgegevens;
- advisering over eventuele melding aan uw relaties;
- advisering over eventuele aansprakelijkstellingen;
- advisering over informatie aan derden.

Dat kan ook technisch zijn, zoals:

- het opsporen en vernietigen van het virus of ander probleem;
- herstellen van databestanden;
- controleren van uw back-up (op bijvoorbeeld virussen);
- veiligstellen van informatie.

Kortom: het incident response-team kan u daadwerkelijk helpen als er iets gebeurt.

Techniek Nederland Verzekeringen

Korenmolenlaan 4
3447 GG Woerden

T 088 543 27 17
E verzekeringen@techniekNederland.nl
W techniekNederland.nl/verzekeringen