Cyber Weerbaarheidscentrum Greenport

Schade van een cyberincident

Dit document bevat informatie over de schade van een cyberincident: Hoe bepaal je de schade van een cyberincident, hoe herstel je deze en hoe doe je de externe communicatie over het incident?

Schade herstellen

Is je bedrijf onverhoopt slachtoffer geworden van een incident? Dan is het zaak om de schade te bepalen. Denk daarbij niet alleen aan daadwerkelijke kosten en verliezen, maar ook bijvoorbeeld de reputatieschade. Ook is het belangrijk dat je als ondernemer de juiste mensen, organisaties en/of instanties informeert. Dit is van belang voor het (terug)-winnen van vertrouwen, maar ook omdat je dit in sommige gevallen verplicht bent.

Schade bepalen van een cyberincident

Ondanks de goede voorbereiding en de maatregelen die je hebt getroffen kun je helaas nog steeds slachtoffer worden van een incident. De schade bepalen van een incident is complex. Niet alleen zal je te maken hebben met directe kosten, maar ook met indirecte kosten. Daarbij is niet alle schade altijd direct vast te stellen, laat staan de hoogte hiervan. Dit kan zijn omdat de gevolgen pas op termijn zichtbaar worden. Bij eventuele reputatieschade kan het zijn dat je na een incident structureel minder bestellingen of opdrachten krijgt. Hieronder vind je een aantal punten waar je aan moet denken bij het bepalen van je schade.

Welke elementen bepalen de kosten van een incident?

De bepaling van de schade in kosten kan je onderverdelen in grofweg de volgende categorieën:

- Directe en indirecte kosten van een incident;
- Directe en indirecte kosten van herstel.

Deze lijst is niet uitputtend. In jouw sector, branche of bedrijf kunnen bepaalde elementen niet van toepassing zijn en andere elementen juist zorgen voor additionele schade en kosten:

Directe kosten van het incident

- Kosten die je maakt om je klanten en leveranciers te informeren;
- Verlies aan (productie-)uren voor je bedrijf;
- Omzetverlies doordat je verkoop van producten of diensten stil ligt;
- Kosten voor crisismanagement en calamiteitenbeheersing.

Indirecte kosten van het incident

- Reputatieschade, klanten en leveranciers kunnen naar een ander bedrijf gaan omdat ze minder vertrouwen hebben in jouw bedrijf;
- Kosten die je maakt om de pers en andere belanghebbenden te woord te staan;
- Boetes van een toezichthouder of autoriteit, bijvoorbeeld een mogelijke boete van de Autoriteit Persoonsgegevens in het geval van een datalek;
- Schadevergoedingen die je moet betalen omdat je (contractuele) verplichtingen niet kan nakomen;
- Verlies van concurrentiegevoelige informatie die anderen kunnen gebruiken, zoals prijzen, contracten en offertes.

Directe kosten van herstel

- Kosten die je maakt voor de inhuur van specialisten om jouw omgeving weer beschikbaar maken;
- Kosten van nieuwe software of hardware indien dit nodig is voor herstel;
- Tijd die je investeert in het opnieuw opbouwen van de inhoud van je systemen en administratie.

Indirecte kosten van herstel

- Opnieuw opbouwen van jouw bedrijfsreputatie bij klanten, leveranciers en derden;
- Training van medewerkers in veilig gebruik van de herstelde, of nieuw gebouwde omgeving.

Uiteraard is het voorafgaand aan een incident lastig de schade vast te stellen. Met bovenstaande punten krijg je hier in ieder geval een beter beeld van.

Het inventariseren van je kwetsbaarheden is belangrijk. Je krijgt daarmee goed inzicht in welke risico's je loopt en welke maatregelen je moet nemen om risico's te beheersen.

Externe communicatie na een incident

Bij het herstellen tijdens of na een incident is het van belang dat je als ondernemer de juiste mensen, organisaties en/of instanties informeert. Dit is van belang voor het (terug)winnen van vertrouwen, maar ook omdat je dit in sommige gevallen verplicht bent. Bij externe communicatie zal je altijd afwegen wat je, aan wie en waarom communiceert. Het kan goed zijn dat het informeren van bijvoorbeeld klanten leidt tot een positieve klantwaardering, maar evengoed kan het zijn dat klanten dit als negatief ervaren. De juiste toon, timing en vorm zijn dus van groot belang.

In onderstaande lijst staan aan aantal categorieën van mensen, organisaties en instanties die je kan (of soms moet) informeren. Dit is geen uitputtende lijst, maar geeft een handreiking om mee te starten. Uiteraard is het aan ieder bedrijf zelf om na te denken of er anderen zijn die ook moeten worden geïnformeerd of dat wellicht partijen die hier genoemd zijn niet van toepassing zijn. Dit kan per incident verschillen.

Tip: een geprinte lijst van belangrijke contacten met namen en telefoonnummers die veilig in een kluis ligt kan een reddingsboei zijn voor de communicatie na een gijzelsoftware aanval.

Personeel

Personeel informeer je over de consequenties van een incident en wat je van hen verwacht in het herstel. Dit kan bijvoorbeeld het verzamelen van informatie zijn. Personeel kan ook worden ingezet bij het verder informeren van klanten en leveranciers. Het personeel kan ook zelf slachtoffer zijn van het incident omdat er bijvoorbeeld persoonsgegevens van hen zijn gelekt. Informeer hen daar dan ook over.

Klanten

Klanten informeer je over de consequenties van het incident die van invloed zijn op de dienstverlening die zij van je verwachten. Denk hierbij aan vertraging van levering van bestellingen, betaling van facturen, afspraken en verzending van offertes. Tevens informeer je klanten over indirecte consequenties voor hen. Bijvoorbeeld als er persoonsgegevens van klanten zijn gelekt. Wanneer je een datalek moet melden en aan wie vind je hier.

Leveranciers

Leveranciers informeer je over de consequenties van het incident die van invloed zijn op de relatie met hen. Bijvoorbeeld wanneer de verwachting bestaat dat zij jouw orders tijdelijk niet leveren, maar ook kunnen orders, contracten of offertes openbaar gemaakt zijn. Ook kunnen er op persoonsgegevens van de leveranciers Autoriteit Persoonsgegevens. Tevens kan het verplicht zijn dat je een melding moet doen bij de branche toezichthouder, denk hierbij bijvoorbeeld aan de Autoriteit Financiële Markten of De Nederlandse Bank. Daarnaast is het mogelijk dat een overheidsdienst voorschrijft dat je een melding moet maken. Een Digital Service Provider (een aanbieder van digitale diensten) zal ook onder bepaalde voorwaarden een melding moeten maken bij het CSIRT DSP.

Contractpartijen en andere partners of belanghebbenden

Contractpartijen zoals klanten en leveranciers, waar contractuele verplichtingen mee zijn aangegaan, kunnen of moeten geïnformeerd worden. Zo kan je met klanten of leveranciers hebben afgesproken dat zij bij een calamiteit worden geïnformeerd, zodat zij passende maatregelen kunnen nemen. Naast deze contractpartijen, kun je ook denken aan bijvoorbeeld partners in de keten. Veel bedrijven maken gebruik van elkaars diensten en soms ook elkaars systemen. Het delen van deze informatie kan toekomstige incidenten voorkomen.

Politie en justitie

Het advies is om bij een cyberaanval altijd aangifte te doen bij de politie. Uiteraard om uit te zoeken wie er achter een aanval zit en om schade uiteindelijk te kunnen verhalen en om te zorgen dat de dader wordt gestraft. Daarbij is er op dit moment nog geen goed beeld van de omvang van cybercriminaliteit in Nederland. Het is niet altijd mogelijk te achterhalen wie jouw bedrijf heeft aangevallen. Jouw aangifte draagt echter wel bij aan de initiatieven die de politie ontplooit om er achter te komen wie er achter zulke aanvallen zit. Een concreet voorbeeld is de bestrijding van gijzelsoftware.

Verzekeraar of bank

Hoewel het fenomeen 'cyberverzekeringen' nog niet wijdverbreid is in Nederland, aldus het verbond van verzekeraars, kan het wel zijn dat het voor jou als ondernemer verstandig is om te overleggen met je verzekeraar of adviseur over het incident en welke maatregelen je moet nemen of welke vergoedingen je kunt ontvangen. Dit geldt ook voor je bank. Wellicht is het nodig om nieuwe passen aan te vragen, de toegang tot internetbankieren te wijzigen of extra alert te zijn op ongebruikelijke transacties.

Adviseurs (derden)

Het informeren van derden zoals externe adviseurs kan ook verstandig zijn. Zoals een boekhouder, accountant, juridisch adviseur of advocaat die kunnen wellicht meedenken in het beperken van de schade.

Samenwerkingverbanden

Als laatste kan het waardevol zijn om samenwerkingsverbanden waarin je participeert te informeren. Je kan hierbij denken aan de specifieke cybersecurity samenwerkingsverbanden die bestaan in Nederland, of aan netwerken zoals ondernemers of brancheverenigingen. Door informatie uit te wisselen kun je andere ondernemers helpen en een steentje bij dragen aan een weerbaar ondernemend Nederland.

Het is van belang om preventief vast te leggen welke personen belangrijk zijn om te informeren indien er een incident plaatsvindt. Het is goed om hier een overzicht van te maken en ook hier gelden onze basisprincipes voor veilig digitaal ondernemen.

Dit document is gebaseerd op de documenten ‘Schade herstellen’, ‘Schade bepalen’ en ‘Externe communicatie na een incident’ van het Digital Trust Center. De originele documenten zijn te vinden via https://www.digitaltrustcenter.nl/informatie-advies/schade-herstellen , https://www.digitaltrustcenter.nl/schade-bepalen-van-een-incident en https://www.digitaltrustcenter.nl/belangrijke-telefoonnummers