Slachtoffer van cybercrime?

Informatie voor het MKB

« waakzaam en dienstbaar »

Criminelen zijn steeds vaker online. Denk aan DDos-aanvallen, ransomware of phishing. Is uw bedrijf slachtoffer geworden? Doe dan direct aangifte en kijk op www.politie.nl voor tips.

In deze folder leest u over het hoe en waarom van aangifte doen. Ook geven we u een beeld van de vormen van cybercrime die we tegenkomen in het MKB en ten slotte geven we u tips om cybercrime te voorkomen.

Waarom aangifte doen?

Op basis van een aangifte kan de politie onderzoek doen, daders zien te achterhalen, meer digitale aanvallen stoppen, andere ondernemers waarschuwen en criminele businessmodellen frustreren. Uw incident kan een relatie hebben met andere zaken, waardoor niet alleen uw eigen zaak mogelijk tot een succesvol eind komt, maar ook die van een ander. Aangifte kan noodzakelijk zijn voor de afhandeling met de verzekering en voor het eisen van een schadevergoeding.

Informeer de politie

Hebt u zelf maatregelen genomen en is uw zaak al opgelost? Laat dit dan ook aan de politie weten, want uw informatie is nuttig voor de politie.
Hetzelfde geldt voor een (mislukte) poging tot een strafbaar feit. Al is uw bedrijf niet daadwerkelijk slachtoffer geworden, er kan wel een goede aanleiding zijn voor nader politieonderzoek.

Hoe doet u aangifte?

Op een politiebureau. Maak hiervoor een afspraak via 0900-8844.

Ter voorbereiding van de aangifte, zorgt u dat degene die namens uw bedrijf aangifte doet daartoe een machtiging heeft. Neem eventuele logbestanden mee (deze bevatten mogelijk sporen, indicaties en bewijzen) en noteer alvast de (contact) gegevens van de aangever.

U kunt de volgende vragen verwachten:

- Welke systemen zijn geraakt?
- Wat zijn de netwerk-infrastructuur en netwerkadressen?
- Welke veiligheidsmaatregelen (zoals virusscanners en firewalls) heeft u genomen?

- Was er een dreigement of waren er andere bijzondere omstandigheden?
- Wat is de geschatte (economische en imago) schade en hoeveel (persoons-)gegevens zijn getroffen?
- Welke (herstel)acties heeft uw bedrijf ondernomen na het ontdekken van het incident?

Wat is cybercrime?

Onder cybercrime verstaan we strafbare feiten die gepleegd worden met ICT-middelen, gericht tegen andere ICT-middelen. Denk aan computers, laptops en servers, maar ook aan tablets, smartphones en andere apparaten met een processor en geheugen die gebruikmaken van internet.

Strafbaar?

Niet alleen de delicten zelf zijn strafbaar, ook het voorbereiden ervan of een poging doen, kan strafbaar zijn.

Vormen van cybercrime

Online slaan criminelen hun slag. Denk aan:

- Zonder toestemming binnendringen in een geautomatiseerd systeem *(hacken)*.
- Installeren of verspreiden van kwaadaardige software *(malware)*.
- Onrechtmatig kopiëren van gegevens, door een hack of door een technisch hulpmiddel te gebruiken.
- Wissen, wijzigen, onbruikbaar of ontoegankelijk maken van gegevens die door een geautomatiseerd systeem zijn opgeslagen.
- Factuur- of CEO-fraude (uitgeven voor een ander)
- Verstoren of ontoegankelijk maken van ICT.

Indicaties van cybercrime

Wanneer moet u alert zijn?

- Als vertrouwelijke gegevens op internet verschijnen.
- In logboeken van uw (web) servers aanvallen staan geregistreerd.
- Systemen van uw bedrijf maken verbinding met verdachte internetadressen.
- Systemen een ongewone activiteit vertonen, zoals extreem hoge belasting.
- Uw systemen zijn gegijzeld en u wordt gevraagd om losgeld te betalen om weer toegang te krijgen tot uw gegevens *(ransomware)*.
- Een concurrent heeft gevoelige bedrijfsinformatie van u in handen.
- De website is verminkt *(defacing)*.
- Bestanden of databases zijn gewist of gewijzigd.
- De website van uw bedrijf is niet langer bereikbaar door grote hoeveelheden inkomend dataverkeer *(DDoS-aanval)*.
- De e-mailserver functioneert niet meer vanwege een grote spamaanval.

- Systemen van uw bedrijf zijn ontoegankelijk gemaakt.
- Er worden onrechtmatig bedragen van uw rekening afgeschreven (als gevolg van phishing of CEO- en factuurfraude). Bij factuur- of CEO-fraude wordt een medewerker altijd onder druk gezet om het geld snel over te maken.
- Er worden onrechtmatig uit naam van uw bedrijf e-mails verstuurd.

Cybercrime bestrijden we samen

Voor het melden van cybercrime kunt u het landelijk telefoonnummer van de politie bellen 0900-8844.

Tips

- Zorg dat uw systemen goed beveiligd zijn en dat u de benodigde updates downloadt en installeert.
- Maak gebruik van een virusscanner, firewall, anti-spyware en advertentieblokkers.
- Bezoek alleen veilige websites. Klik niet op onbekende bestanden en links.
- Is een rekeningnummer veranderd naar een buitenlandse bank? Neem dan contact op met de facturerende partij via een voor u bekend telefoonnummer of mailadres en niet via het genoemde nummer of mailadres in de mail. Bespreek deze afspraak met de financieel medewerkers. Spreek een maximum bedrag af dat door de medewerker zonder controle van een andere persoon mag worden overgemaakt.
- Gebruik sterke wachtwoorden, liefst wachtzinnen.
- Maak regelmatig een back-up.
- Log gebeurtenissen op systemen.
- Informeer uw personeel over deze digitale dreigingen. Veel malware wordt binnengehaald doordat medewerkers vaak privé e-mails of bestanden openen in de werkomgeving,

Loggen

Het loggen van gebeurtenissen helpt om cybercrime snel te ontdekken en meteen in te kunnen grijpen. Ook helpt het de politie om de daders te achterhalen. Bijna alle systemen binnen een bedrijf kunnen logboeken genereren over netwerkactiviteiten, zoals inlogpogingen en toegang tot bestanden.

Aanvallers zullen vaak proberen om logboeken te verwijderen. Het is daarom aan te raden om logboeken binnen uw bedrijf centraal op een beveiligde server op te slaan. Maak beleid voor de bewaartermijnen van loggegevens. Houd daarbij rekening met het feit dat digitale inbraken soms pas maanden later worden ontdekt. Ook een onderzoek kan enige tijd in beslag nemen, waardoor loggegevens door (automatische) vernietiging verloren kunnen gaan.

Naast de politie houden diverse organisaties zich bezig met het bestrijden en voorkomen van cybercrime. Ook bij hen kunt u terecht voor tips, informatie en ondersteuning.

Voor anonieme meldingen kunt u terecht bij **Meld Misdaad Anoniem**, telefoonnummer 0800-7000.

De Koninklijke Marechaussee (**KMar**), onder meer verantwoordelijk voor de politietaak op luchthavens en defensieterreinen, is te bereiken op nummer 0800-1814.

De Algemene Inlichtingen- en Veiligheidsdienst (**AIVD**) onderzoekt cyberspionage, complexe cyberaanvallen die de nationale veiligheid bedreigen. Zie www.aivd.nl

De Autoriteit Persoonsgegevens (**AP**) houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens. Als bij een cybercrime-incident persoonsgegevens zijn geraakt, kan uw bedrijf verplicht zijn om dit te melden. Raadpleeg hiervoor de website www.autoriteitpersoonsgegevens.nl.

De Fraudehelpdesk is in Nederland een centraal punt voor vragen, informatie en meldingen over fraude en oplichting en verwijst slachtoffers door naar de juiste instantie. De Fraudehelpdesk ondersteunt particulieren en ondernemers. Zie www.fraudehelpdesk.nl

De **Autoriteit Consument en Markt** houdt toezicht op het consumentenrecht, mededingingsrecht en enkele specifieke sectoren, waaronder telecommunicatie. Naleving van regels over spam vallen daaronder. Via de website www.acm.nl kunnen klachten gemeld worden. Anoniem melden, kan ook. Consumenten kunnen terecht op www.consuwijzer.nl. Klachten over spam kunt u melden via www.spamklacht.nl.

Financieel dienstverleners, zoals banken, hebben vaak een **contactlijn** of loket waar u incidenten zoals fraude of diefstal kunt melden.

www.politie.nl

« waakzaam en dienstbaar »

18226