WEBINTENSE SECURITY PAPER

Digitale Beveiliging

Stappenplan voor de beveiliging van je gegevens. Wat moet je doen als je gehackt bent?

WebIntense BV Hanninkhoek 42, 7546AA Enschede, KVK: 70647666,
BTW: NL858407073B01, Bank: NL53KNAB0257031685 mail: info@webintense.nl

INHOUD

INLEIDING

Mkb steeds vaker doelwit cybercriminelen

Wereldwijd verschijnen er 30 nieuwe malware programma's per seconde (bron: Symantec). Daarnaast neemt het aantal database-inbraken toe, terwijl onderzoek van Digibewust aangeeft dat één op de 10 Nederlanders wel eens is gehackt.
In tegenstelling tot wat vaak wordt aangenomen, blijkt dat het mkb wel degelijk interessant is voor hackers. Sterker nog, het mkb is zelfs steeds vaker doelwit.
De cijfers wijzen uit dat het daarbij niet zozeer gaat om de grootte van bedrijven, maar vooral om een zo groot mogelijk aantal slachtoffers. Cybercriminelen gaan voor volume, in plaats van kwaliteit.
Hoewel de wetgeving op het gebied van cybersecurity nog altijd wordt aangescherpt, biedt dat geen garantie dat u verlost bent van schadelijke software.
Kortom, alle reden om de beveiliging van het computernetwerk van uw bedrijf eens kritisch tegen het licht te houden. Daarbij zult u, net als in de fysieke wereld, bepaalde maatregelen moeten nemen om te voorkomen dat uw bedrijfsgegevens worden gestolen.
Dit document biedt u een handleiding voor het optimaliseren van de beveiliging van uw computersysteem en netwerk. Het heeft echter niet de pretentie dé allesomvattende oplossing te bieden waarmee u uw veiligheidsproblemen in een keer oplost.

1. ZO BEVEILIGT U UW BEDRIJFSGEGEVENS:

A.Maak een risicoanalyse

- **Maak, in samenwerking met een ervaren online beveiligingsspecialist, een risico-analyse: Welke onderdelen van uw bedrijfsvoering vormen een potentieel risico op ICT-gebied?**
- **Denk aan desktops, laptops, smartphones en tablets, e-mail, internettoegang, databases? Waar 'staat' belangrijke bedrijfsinformatie? Is die informatie goed beveiligd? Laat de**
- **huidige beveiliging testen door een specialist. Welke software kan de risicovolle onderdelen optimaal beveiligen? Kijk, in plaats van alleen 'losse' producten, ook naar geïntegreerde oplossingen. Die zijn vaak voordeliger, overzichtelijker en veiliger. Vraag offertes aan en nodig de beste drie uit voor een demo.**

B. Kies de juiste beveiliging

- **Kies voor een beveiligingsproduct dat goed bij het bedrijf past én overzichtelijke en begrijpelijke rapportages geeft.**
- **Vergelijk verschillende producten en betrek een specialist bij de uiteindelijke keuze. Evalueer regelmatig de gekozen beveiligingsoplossing: past die nog wel bij de huidige én de toekomstige situatie?**
- **Vergeet ook niet om een goede verzekering af te sluiten, die eventuele computervredebreuk dekt.**

C. Voorlichting aan medewerkers

- **Licht medewerkers voor over potentiële risico's van bijvoorbeeld (eigen) laptops, smartphones en tablets die ze voor het werk gebruiken.**
- **Overweeg de aanschaf van een beveiligingsproduct voor mobiele apparaten waarmee bijvoorbeeld een verloren of gestolen laptop of smartphone op afstand buiten werking gesteld kan worden.**
- **Maak medewerkers duidelijk dat het 'zomaar' klikken op links in e-mails risicovol is.**
- **Bespreek de gevaren van social engineering (zie begrippenlijst).**
- **Zorg dat uw medewerkers regelmatig hun wachtwoorden moeten wijzigen en stimuleer het gebruik van sterke wachtwoorden.**

Kortom: zorg voor een helder internet- en e-mailbeleid.

2. BENT U GEHACKT? HERKEN DE EERSTE TEKENEN

Onderstaande situaties kunnen een signaal zijn dat uw systeem gecompromitteerd is, of dat een hacker probeert toe te slaan.

A. Verdachte telefoontjes, e-mails en usb-sticks
Hackers richten zich vaak op de zwakste schakel in de beveiliging: de mens. Ze proberen iemands vertrouwen te winnen, in de hoop dat diegene zich dan niet aan de normale veiligheidsprocedures houdt en gevoelige gegevens prijsgeeft. Dit kan bijvoorbeeld via een telefoontje ("Hoi, ik ben Joost van IT. Ik heb gehoord dat je computer traag is. Ik wil je graag helpen, maar dan heb ik wel even je gebruikersnaam en wachtwoord nodig.") of een e-mail. Maar het kan ook gaan om een usb-stick die "toevallig" op de balie ligt en spyware of een Trojan bevat.

B. Ongewone activiteit in logbestanden
Het goed interpreteren van logbestanden kan een zware, specialistische taak zijn. Een firewall en antivirus-software met intelligente monitoring kan daarbij veel werk schelen. De beheerder krijgt dan bericht bij verdacht gedrag of patronen.

C. Problemen met accounts
Wanneer een gebruiker verschillende keren niet op normale wijze kan inloggen op een account, dan kan dat betekenen dat iemand anders heeft geprobeerd in te loggen. Tevens wordt er, op bijvoorbeeld phishing-pagina's, een nep-inlogvenster gebruikt dat doorlinkt naar een legitieme website. Of er komt een melding dat de inloggegevens onjuist zijn, waarna ze opnieuw ingevoerd worden. De cybercrimineel krijgt zo toegang tot deze gegevens.

D. Problemen met servers en/of capaciteit
Een DdoS-aanval (Distributed Denial of Service) houdt in dat er zeer veel dataverkeer wordt gegenereerd om een server offline te halen. Hiervoor circuleren verschillende tools, die bijvoorbeeld proberen een website meerdere keren in te laden. Dit gebeurt dan zo massaal, dat de machine daarachter het niet meer aan kan. In sommige gevallen geeft dit extra aanvalsmogelijkheden (vectoren, zie begrippenlijst), door misbruik te maken van crashende applicaties.

3. DE 10 STAPPEN DIE U MOET ZETTEN NA EEN HACK

Is uw bedrijf gehackt, of is er een vermoeden dat dit is gebeurd? Schakel dan zo snel mogelijk een online beveiligingsspecialist in. Schakel het gehele bedrijfsnetwerk, ook internet en wifi, volledig uit. Heeft u tools nodig om de infectie op te lossen, haal die dan binnen via een computer die niet met uw netwerk is verbonden.

Stap 1: Reageer snel en doe aangifte
Een snelle reactie kan reputatieschade enorm beperken. Huur, als u deze kennis niet zelf in huis hebt, een gespecialiseerd bedrijf in om uw computersysteem te laten onderzoeken. Doe tevens aangifte (zie onder) van computervredebreuk, internetoplichting of fraude.

Stap 2: Noteer wat u doet, denk aan mogelijke juridische gevolgen
Het is niet ondenkbaar dat andere partijen juridische stappen nemen tegen uw organisatie. Om een goede verdediging op te bouwen, is het belangrijk dat u kunt aantonen welke keuzes u heeft gemaakt en op basis van welke gegevens.

Stap 3: Stel uw netwerk veilig
Voorkom dat de hack zich verder uitbreidt, of dat waardevolle gegevens alsnog gekaapt kunnen worden van uw netwerk. Zorg dat openstaande verbindingen naar andere kantoren of thuiswerkers, zo snel mogelijk worden afgesloten. De omvang van de hack of virusuitbraak blijft daardoor onder controle.

Stap 4: Professionele, eenduidige communicatie
Zodra de pers hoort over de inbraak, gaat ze op zoek naar een verhaal. Zorg dat u dat voor die tijd al klaar hebt, en dat uw informatie naar de pers toe eenduidig is.

Stap 5: Bepaal de omvang van de inbraak
Wat is de omvang van de gegevensinbraak? Zet dat op een rij. Welke systemen zijn gecompromiteerd, welke gegevens zijn gelekt en identificeer de herkomst. Het motief van de hacker(s) is hierbij zeker van belang.

Stap 6: Informeer stakeholders
Informeer snel alle stakeholders, eventueel via de pers. Een tekst op uw site of een mail naar uw klanten is soms al voldoende. Hou het kort, bondig en eenduidig. Rectificatie is onwenselijk, dat maakt het lastig om te begrijpen wat er aan de hand is. Uw betrouwbaarheid is geschaad, zorg dat uw verhaal betrouwbaar is en blijft!

Stap 7: Voldoe aan eventuele meldplichten
De Nederlandse wetgeving kent verschillende meldplichten in het geval van een hack. Zorg dat u altijd melding doet bij de juiste instanties. Laat u eventueel door een jurist adviseren: bij welke instanties u verplicht bent om melding te doen van de gegevensinbraak?

Stap 8: Vervang alle wachtwoorden
Deze stap lijkt vanzelfsprekend, maar wordt nog wel eens vergeten. Vervang ál uw wachtwoorden! Dus niet alleen die van uw gebruikers, maar ook van serviceaccounts en beheeraccounts.

Stap 9: Vervang certificaten
Als een hacker uw certificaten in handen heeft gekregen kan hij hiermee uw gegevens aftappen, ook al lijken deze veilig. Dit geldt zeker als u een webshop heeft! Zorg er tevens voor dat uw oude certificaten als onbetrouwbaar worden aangemerkt bij uw certificaatverlener.

Stap 10: Evalueer
Evalueer wat er is gebeurd. Pas uw beleid aan waar het tekort is geschoten. Verhoog uw beveiligingsniveau en verlaag de kans op toekomstige hacks. Laat daarna uw netwerk testen door een gespecialiseerde organisatie, zodat u de veiligheid van uw informatie kunt waarborgen.

Aangifte en meldplicht

Computervredebreuk, de juridische term voor hacken, is strafbaar volgens het Wetboek van Strafrecht. Hiervan kunt u aangifte doen bij de politie, bijvoorbeeld via Mijn Politie. Er is sprake van computervredebreuk wanneer iemand opzettelijk en zonder toestemming binnendringt in het computersysteem of netwerk van een ander. Kijk hier voor meer informatie.
Bent u een aanbieder van een informatiedienst, dan moet u diefstal, verlies of misbruik van gegevens melden. Meer info op de website van het College Bescherming Persoonsgegevens.

4. GEVOLGEN VAN HACKING

**Hackers dringen computers binnen om te stelen of om andere illegale zaken te verrichten.
De hacker wil wachtwoorden van de eigenaar van de computer te weten komen en toegang krijgen tot bijvoorbeeld bankaccounts, inlognamen en wachtwoorden van documenten waarin belangrijke bedrijfs- of klantinformatie staat.
Op de gehackte computer kunnen bestanden worden gezet, die weer door andere cybercriminelen gebruikt worden.
Het misbruiken van ruimte op de computer of website voor het uitvoeren van aanvallen op andere computers of het platleggen van websites van bedrijven of organisaties, die daar mogelijk schade door ondervinden.
De hacker kan een programma op een computer installeren waardoor de computer spamberichten (agressieve reclame) gaat versturen. Op grote schaal spamberichten versturen is strafbaar. Als spam dus vanaf een andere pc afkomt, dan loopt de hacker geen groot risico om bestraft te worden.
Schades veroorzaakt door hackers komen juist vaak bij kleinere ondernemingen hard aan, omdat er minder (financiële) ruimte is om klappen op te vangen.**

A. Financiële schade

Storingen in e-mail of internet, zoekgeraakte gegevens en het herstellen van de schade aan computers en netwerken ten gevolge van cybercrime zijn vaak kostbaar.

B. Imagoschade

Bijvoorbeeld: het ongewild versturen van spam en gegevens die openbaar worden gemaakt, kunnen negatieve publiciteit creëren en het imago schaden.

C. Identiteitsdiefstal

Identiteitsdiefstal is diefstal van persoonlijke gegevens. Vaak vindt identiteitsdiefstal plaats om financiële redenen, maar er kunnen ook andere motieven zijn voor deze vorm van criminaliteit.

D. Diefstal van data

**Denk aan administraties, offertes, e-mails en bankrekeningnummers die worden gestolen.
Deze informatie kan worden gebruikt voor diefstal van geld of voor chantage. Daarnaast gebeurt het ook dat informatie wordt doorverkocht aan andere criminele organisaties of andere 'geïnteresseerden'.**

5. BEGRIPPENLIJST

Cybercrime
Vorm van criminaliteit die betrekking heeft op computersystemen (inclusief netwerken)

DDoS-aanval
DDoS staat voor Distributed denial-of-service. Aanvallen worden gepleegd vanaf meerdere computers. Er wordt geprobeerd om een computer, computernetwerk of dienst onbruikbaar te maken.

Firewall
Een firewall is een systeem dat een netwerk of computer kan beschermen tegen misbruik van buitenaf.

Hacker
Een hacker is in het dagelijks spraakgebruik meestal iemand die illegaal inbreekt in computersystemen. Er zijn echter ook goedwillende hackers, bijvoorbeeld om de beveiliging van een site te verbeteren.

Infectie, virus
Er wordt gesproken over een infectie wanneer een computer ten prooi is gevallen aan bijvoorbeeld een computervirus.

Malware
Malware is een verzamelnaam voor kwaadaardige en/of schadelijke software. Het woord is een samenvoeging van het Engelse 'malicious software'.

Phishing
Een verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Phishing vindt vaak plaats per e-mail. De afzender doet zich dan voor als een betrouwbare zakenrelatie (bijv. uw bank).

Poortscan
Een poortscan controleert welke computer poorten er open staan voor internetverkeer. Applicaties maken gebruik van poorten om over te communiceren

Social engineering
Social engineering is een techniek waarbij een hacker de zwakste schakel in de beveiliging, de mens, benadert. Het doel is om vertrouwelijke of geheime informatie los te krijgen, zodat de hacker dichter bij het aan te vallen object kan komen.

Spyware
Spyware zijn (delen van) computerprogramma's die informatie vergaren over gebruikers en doorsturen naar een externe partij. Het doel is meestal om geld te verdienen.

Trojan
Een Trojan, ofwel Trojaans paard, is een functie die in een programma verborgen zit en kwaadwillenden toegang geeft tot de computer.

Vector
Een (aanvals)vector is de methode die malware gebruikt om zichzelf te verspreiden of een computer te besmetten.