Whitepaper: ***Online*** merkbeveiliging

eFuture

Stationsplein 12 - 1 | 1211 EX Hilversum | +31 (0) 35 531 1115

Bescherm je merk- en klantgegevens online

Merkbescherming online doe je door jouw merk, productnamen en daarnaast logo's te laten registreren en door belangrijke domeinnamen vast te leggen. Maar er zijn ook andere zaken die een merk kunnen schaden. Dit whitepaper geeft je tips om merk -en klantgegevens online te beschermen.

Je kunt ervan uit gaan dat de beveiliging van externe leveranciers (zoals een ESP) op orde is. Je krijgt een account aangeleverd, met één of meerdere gebruikersaccounts waar je altijd en overal toegang tot hebt. Maar wat zou er gebeuren als deze gebruikersaccounts in handen van een kwaadwillende zouden vallen?

Je klantendatabase kan dan op straat belanden met alle gevolgen van dien. Het is zeer kostbaar om een goede klantendatabase op te bouwen. Ga maar na welke kosten je al hebt gemaakt om dit te bereiken. Juist daarom is het voor criminelen interessant om bij een database in te breken. Als dit (mogelijk) gebeurt spreken we van een datalek.

Wees bewust

Veel medewerkers zijn zich er vaak niet van bewust dat gevoelige info op een eenvoudige manier al gelekt kan worden. Het is dan ook van groot belang dat er wordt gewerkt aan de bewustwording van de risico's die datalekken met zich meebrengt. Iedereen binnen de organisatie dient te weten wat de risico's zijn, maar ook wat de meest ideale werkwijze is om met gevoelige informatie om te gaan. Denk aan vragen als: Wat te doen bij diefstal/verlies van laptop, pc, USB-stick of smartphone? En wat is de gewenste werkwijze indien gevoelige info wel gedeeld dient te worden?

Hieronder tips die meegenomen kunnen worden bij het verlenen van toegang tot essentiële data:

1

Opslag bestanden

Waar worden bestanden opgeslagen? Indien het niet nodig is dat bestanden op een laptop staan, verwijder deze dan! Zo minimaliseer je de kans op een lek.

2

Veilige werkplek

Indien de werkplek verlaten wordt is het aan te raden om de pc/laptop te vergrendelen.
Je weet immers nooit wat er gebeurd indien je zelf niet aanwezig bent.

3

Benader het systeem altijd via HTTPS

Het gebruik van een beveiligde verbinding die je gegevens versleutelt zorgt ervoor dat deze onleesbaar worden voor derden.

4

Gebruik aanvullende beveiligingsmethoden (twee staps authenticatie)

Vaak is het mogelijk om een aanvullende beveiligingsmethode in te stellen. Bij het gebruik van 'twee staps authenticatie' wordt de identiteit van een gebruiker ook op een alternatieve manier bevestigd.

5

Verstuur een database nooit per mail

Het is belangrijk om een database nooit per mail te versturen aan externe leveranciers. Lever dergelijke bestanden aan via een beveiligde verbinding om te voorkomen dat ze ergens in een inbox of outbox blijven staan.

6

Gebruik unieke user accounts (met bijbehorende rechten) per gebruiker

Door het gebruik van een uniek account voor elke gebruiker wordt het eenvoudiger om roulering in medewerkers te verwerken. Je geeft een stagiair alleen de rechten die hij/zij nodig heeft en als de stage periode is afgerond, kan de gebruiker in het systeem direct worden verwijderd (neem dit ook op huidige procedures). Denk ook goed na wie er toegang moeten hebben, en probeer dit aantal te beperken.

7

Wachtwoord policies

Het is goed om binnen een organisatie wachtwoord policies te definiëren. Verplicht medewerkers tot het gebruiken van sterke wachtwoorden en laat ze deze wachtwoorden ook regelmatig vernieuwen. Tips: gebruik geen namen, data en wees creatief met hoofdletters, kleine letters, cijfers en symbolen. Een hele zin is doorgaans gemakkelijker te onthouden dan losse tekens.

8

Voorkom misbruik van je domein

Naast banken en financiële instellingen worden steeds vaker ook andere bedrijven getroffen door 'phishing'. Hierbij wordt er spam verstuurd naar willekeurige adressen en worden de ontvangers verleid tot het achterlaten van privacy gevoelige informatie.

Je kunt zelf actie ondernemen om phishing te voorkomen. Implementeer DMARC om misbruik van je domein te voorkomen en phishing mails te blokkeren. Lees verder voor een uitgebreide toelichting: *www.dmarcanalyzer.com* of neem contact met ons op!

9

Toegang tot wifi

Vermijd websites waar je dient in te loggen. Gebruik bijvoorbeeld VPN. Schakel wifi alleen in wanneer dit strikt noodzakelijk is.

10

Stel een datalekprotocol op

Zorg ervoor dat je niet hoeft te improviseren wanneer het feit van een datalek daar is. Een datalekprotocol zorgt ervoor dat de juiste mensen op het juiste moment worden geïnformeerd en handelen waar nodig.

Meldplicht datalekken

Mocht er onverhoopt toch sprake zijn van een datalek binnen de organisatie, dien je dit te melden bij de Autoriteit Persoonsgegevens. Sinds 1 januari geldt namelijk de Meldplicht Datalekken. Het fenomeen 'datalek' is breed gedefinieerd. Daardoor krijg je al snel met de meldplicht te maken. De wet spreekt van een datalek wanneer *persoonsgegevens verloren raken of onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten.* Wat valt hieronder? Het aanpassen en/of veranderen van persoonsgegevens en onbevoegde toegang tot, of afgifte daarvan.

Er is dus niet alleen sprake van een datalek als een hacker toegang tot persoonsgegevens krijgt. Ook verlies van een USB-stick in de trein, of het sturen van een mailing met adressen in het CC-veld (in plaats van het BCC-veld) telt al als datalek. En zelfs verlies van gegevens zoals bij een brand in het datacentrum terwijl er geen back up beschikbaar is, ziet de wet als een datalek.

In alle gevallen is voorkomen natuurlijk beter dan genezen. Anders gezegd, zorg ervoor dat de beveiliging van de gegevensverwerking op orde is. En wees voorbereid op de situatie dat er toch een datalek ontstaat.

Ook het beste uit je online marketing halen?

eFuture is een gedreven online marketing organisatie. Met proactieve en persoonlijke begeleiding, helpen wij bedrijven met vraagstukken op het gebied van E-mailmarketing, Search Engine Marketing, Website Optimalisatie, Social Media Marketing en Online Viral Campagnes. Met ons in huis ontwikkelde e-mailmarketing platform eFuture Engine verzenden wij dagelijks miljoenen e-mailnieuwsbrieven en servicen wij onze klanten met succes.

Neem contact met ons op via ***info@efuture.nl*** *of* ***+31 (0)35 531 1115***

www.efuture.nl