Qweb

A TECHONE COMPANY

HOSTING - NIEUWS

NIS2

WAT BETEKENT DIT VOOR JOU?

Nieuwe Europese wetgeving actief vanaf 2024

1 MEI

SECURITY BASELINE
Is de basis hygiëne op orde?

JOUW DATA IN ONS BEHEER
Wie is er verantwoordelijk wanneer het fout gaat?

info@qweb.nl - 0882 088 088 - qweb.nl

NIS2

WAT BETEKENT DIT VOOR JOU?
NIEUWE EUROPESE WETGEVING ACTIEF VANAF 2024

We ontkomen er niet aan, de NIS2 (Network and Information Systems 2), dé nieuwe Europese wetgeving voor cyberbeveiliging die vanaf 2024 van kracht wordt en ook van toepassing gaat zijn op de hostingbranche. Het doel van deze nieuwe wetgeving is om beveiliging van netwerken en informatiesystemen, van onder anderen hostingproviders, in de EU te versterken en cyberaanvallen te voorkomen of de gevolgen daarvan te beperken. Volgens de NIS2-wetgeving zijn hostingproviders verplicht om passende maatregelen te nemen om hun cyberbeveiliging te verbeteren en om incidenten onmiddellijk te melden bij de nationale autoriteiten. De wetgeving legt tevens strengere sancties op wanneer er niet wordt voldaan aan de gestelde eisen. Maar wat houdt deze nieuwe wetgeving nu precies in en hoe gaat jouw provider ervoor zorgen dat aan alle eisen wordt voldaan? En hoe kan jij er zelf voor zorgen dat jij met jouw bedrijf voldoet aan de nieuwe regelgeving?

SECURITY BASELINE

IS DE BASIS HYGIËNE OP ORDE?

Digitalisering is mooi en ontwikkeld zich razendsnel. Toch brengt het ook de nodige gevaren met zich mee. Zo kunnen wij tegenwoordig overal en op ieder tijdstip hybride werken. Maar hoe zit het dan met de (online) veiligheid? Als we overal en nergens werken wordt het voor de ICT-beheerder moeilijker om om te gaan met de security. Je hebt als het ware 20% aan zicht en 100% aan gevaren. Het is lastig om alle medewerkers goed in de gaten te houden en om te controleren of zij zich houden aan de securityregels. Ondernemers en bedrijven zijn dan ook wel degelijk interessant voor cybercriminelen. De ondernemer gaat lekker aan het werk en heeft allerlei soorten software, maar deze software bevat vaak veel fouten. De basis hygiëne is dan ook vaak niet op orde. Zo wordt er veelal geen gebruik gemaakt van 2FA, er worden slechte wachtwoorden ingezet en er ligt geen plan op tafel voor wanneer er iets fout gaat. Zorg er dus in ieder geval voor dat de basis hygiëne altijd op orde is. En zorg uiteraard voor een plan voor wanneer er toch iets mis dreigt te gaan. Voorkomen is immers altijd beter dan genezen.

JOUW DATA IN ONS BEHEER

WIE IS ER VERANTWOORDELIJK WANNEER HET FOUT GAAT?

In de IaaS markt ontstaat weleens discussie over wie verantwoordelijk is voor de beveiliging van het geheel. Een ICT-leverancier huurt een stuk infrastructuur, en richt dat vervolgens op een bepaalde manier om het daarna aan de eindklant aan te bieden als een ICT-omgeving. Om niet in een discussie terecht te komen over de schuldvraag en aansprakelijkheid is het verstandig om duidelijk te zijn in wat je wél levert, maar ook vooral in wat je niet levert. Bespreek alle mogelijkheden en consequenties met de klant én zet gemaakte afspraken ook op papier.

In het geval van een hack waarbij gegevens worden gecompromitteerd, kunnen zowel de ICT-leverancier als de eindgebruiker verantwoordelijkheden hebben, afhankelijk van de oorzaak van de hack, de aard van de gegevens en de specifieke omstandigheden.
ICT-leverancier: De ICT-leverancier kan verantwoordelijk worden gehouden als de hack het gevolg is van een beveiligingslek in hun product of dienst dat zij hadden moeten verhelpen of voorkomen. Bijvoorbeeld, als de hack het gevolg is van een bekende kwetsbaarheid in de software van de ICT-leverancier die niet op tijd is gepatcht, kan de ICT-leverancier aansprakelijk worden gesteld voor het nalaten van adequate beveiligingsmaatregelen.
Eindgebruiker: De eindgebruiker kan verantwoordelijk worden gehouden als de hack het gevolg is van onvoldoende beveiligingsmaatregelen aan hun kant. Bijvoorbeeld, als de eindgebruiker zwakke wachtwoorden heeft gebruikt, toegangsrechten onjuist heeft beheerd, of nalatig is geweest in het implementeren van beveiligingsupdates, kan de eindgebruiker medeverantwoordelijk worden gehouden voor het datalek.
Het is belangrijk om te benadrukken dat de verantwoordelijkheden in geval van een hack vaak afhankelijk zijn van diverse factoren, waaronder de geldende wet- en regelgeving, contractuele afspraken tussen de ICT-leverancier en de eindgebruiker, de aard van de gegevens en de omstandigheden van de hack. In sommige gevallen kunnen zowel de ICT-leverancier als de eindgebruiker aansprakelijk worden gesteld, en de uiteindelijke beoordeling kan worden gemaakt door juridische instanties op basis van de specifieke feiten en omstandigheden van het geval. Het is belangrijk voor zowel ICT-leveranciers als eindgebruikers om passende beveiligingsmaatregelen te implementeren en te voldoen aan de geldende wet- en regelgeving om het risico van een hack en de mogelijke gevolgen te minimaliseren.

PRODUCT VAN DE MAAND

DAGELIJKSE BACK-UP

Met de dagelijkse back-up van Veeam zorgen wij voor een dagelijkse back-up van jouw website/server. Is jouw website gehackt en/of zijn jouw gegevens verloren gegaan waardoor jij een back-up nodig hebt? Geen probleem. Wij hebben direct een recente back-up beschikbaar.

Neem voor meer informatie over die product contact op met onze helpdesk.

QWEB NIEUWS

Deze maand mocht Techone de cybersecurity partij Treadstone verwelkomen in de groep.

In Treadstone hebben wij een nieuwe partner gevonden waarmee wij kunnen sparren op het gebied van cybersecurity. Wij kijken uit naar deze samenwerking en zullen het komende jaar meer bekend maken over de gemaakte ontwikkelingen op het gebied van online veiligheid.

ThreadStone CYBER SECURITY

Qweb