
MITE3
CYBERSECURITY
226.34
Mighty Security is what we do

Over ons

Bij MITE3 Cybersecurity creëren wij een realistisch inzicht in de digitale veiligheid van uw onderneming. Wij zorgen ervoor dat u met een duidelijk en in mensentaal te begrijpen advies uw informatiebeveiliging naar een hoger niveau kunt tillen.

En wij doen dat met zeer ervaren, getrainde en vooral ook bevlogen cybersecurity experts. De wereld van informatiebeveiliging is complex en vraagt veel specialistische kennis. Laat ons daarom u helpen om eenvoud en duidelijkheid te creëren in deze wereld. Laat onze passie voor het vakgebied de vangrail voor uw organisatie zijn.

Dan kunt u eindelijk eens echt genieten van het ondernemen en uw vrije tijd.

Kwetsbaarheden-scans

Heeft u een website, cloudservice of IT-infrastructuur waarvan u de beveiliging wilt laten scannen of testen? Wij kunnen voor u een kwetsbaarheidsscan en -assessment of een pentest uitvoeren. Hiermee onderzoeken we of de ingrediënten voor het ‘recept’ van een hack of datalek aanwezig zijn. Op basis van de bevindingen helpen we u ook om de gevonden problemen te verhelpen.

Pen-tests

Wilt u weten of een specifieke beveiligingsmaatregel, website of IT-infrastructuur kan worden doorbroken? Om deze vraag te beantwoorden kunnen we een pentest uitvoeren. Een kwetsbaarheidsscan is voornamelijk geautomatiseerd, maar met een pentest zullen we zelf verschillende hacker-tools handmatig gebruiken. Met deze verschillende hacker-technieken testen we dus echt de weerbaarheid van uw veiligheidsmaatregelen.

Open Source Intelligence

Open Source Intelligence (OSINT) en Social Media Intelligence (SOCMINT) zijn onderzoeksmethoden voor het verzamelen van informatie uit openbare bronnen. Denk aan internet, sociale media, de bibliotheek en andere vormen van openbaar beschikbare informatie. Dit kan gaan van een 'due diligence'-onderzoek tot en met het vinden van fraudeurs die actief zijn in uw webwinkel.

Social Engineering

Social engineering is de praktijk, of eigenlijk de kunst, om informatie van mensen te krijgen. Een Social Engineering-test kan erg handig zijn om te testen of uw security awareness campagnes echt werken. Geeft uw HR-afdeling gewoon BSN-nummers telefonisch door? Of vertelt uw IT-engineer of er problemen zijn? Wij gaan het voor je uitzoeken!

We kunnen deze vaak onbewuste manier van lekken van data onderzoeken en dat helpt je om je bewustwordingstraining een boost te geven.

Proactieve Fraude onderzoek

Wanneer bedrijfsprocessen of ICT financiële verleidingen kennen, kunt u snel het slachtoffer worden van fraude of andere vormen van cybercriminaliteit.

Met onze kennis en expertise op het gebied van de vele verschillende vormen van fraude kunnen wij u helpen bij het onderzoeken van de kwetsbare gebieden in uw bedrijf. Op basis van ons advies kunt u vervolgens gerichte maatregelen nemen om het risico op fraude en cybercriminaliteit effectief te verminderen of zelfs te elimineren.

Fraude Incident onderzoek

Helaas is het gebeurd, de ‘portemonnee’ van uw bedrijf is beroofd. U bent misschien opgelicht door CEO-fraude, online verkoop fraude of misschien op een andere manier.

Wij kunnen u helpen onderzoeken wat er is gebeurd en waar het mis is gegaan. De focus ligt hier niet per se op het vinden van de dader, maar op het leren wat er mis is gegaan. Op basis van die lessen kunnen we u adviseren welke maatregelen herhaling kunnen voorkomen.

Advies

Wilt u advies op het gebied van Informatiebeveiliging, Cybersecurity, Privacy, IT, technologie of een ander denkbaar onderwerp dat iets met IT of Cybersecurity te maken heeft? Wij kunnen u immers ondersteunen en voorzien van het juiste advies over een breed scala aan onderwerpen, vragen en problemen.

Op weg naar de Cloud

U wilt naar de Cloud, maar weet niet hoe. Het kan immers moeilijk zijn om grip te krijgen op Cybersecurity terwijl u naar de Cloud gaat. Wij kunnen u zelfstandig helpen bij het selecteren van een oplossing die past bij uw probleem of probleem. En daarbij kijken we nadrukkelijk naar veiligheid, privacy en onderhoudbaarheid.

Dus begin met onze hulp met uw Cloud-ervaring met een sterke Cybersecurity!

Van de Cloud in de drup

U heeft (een deel van) uw omgeving in de Cloud of uitbesteed aan een partner of leverancier. Wat een tijdje goed ging, werd later suboptimaal of minder voorspelbaar. U heeft geen inzicht in de cyberrisico's, dreigingen en kwetsbaarheden en het is onduidelijk wat de Cybersecurity status van uw Cloud is

Pak dus niet de paraplu, maar zorg ervoor dat uw Cloud stopt met regenen met onze hulp.

Onze contact informatie

Adres	Holtackers 14
Postcode	7824 LB
Provincie	Drenthe
Stad	Emmen
Telefoon	085 0290 572
Website	www.mite3.nl
E-mail	info@mite3.nl

Onze financiele details

KVK	71698892
BTW	NL858814973B01
IBAN (ING Bank N.V.)	NL51 INGB 0008 3127 78
Ten name van	MITE3 Cybersecurity
BIC / SWIFT	INGBNL2A

Onze bedrijfsinformatie

MITE3 Cybersecurity is opgericht door Joram Teusink (Teusink.eu Holding B.V. – 71685758), Hans Minten (Hans Minten B.V. 71684417) en Maarten Minten (Maarten Minten B.V. 71684395) op 18 mei 2018.

MITE3 Cybersecurity, MITE3 en MITE3 Security zijn geregistreerde handelsnamen van Digicy.Cloud B.V. te Emmen, Kamer van Koophandel 71698892.

MITE3 Cybersecurity gaat als woordmerk (1419126) en beeldmerk (1419127) beschermd worden in de Benelux (België, Nederland, Luxemburg).