CyberContract

PREVENTIE

Cybercontract biedt bedrijven toegang tot een unieke set gespecialiseerde diensten bij lokale professionals !
Diensten van bewezen kwaliteit … snel en centraal toegankelijk. Zo helpen we u héél concreet bij de uitwerking van een goed preventieplan rond cyber-incidenten. Preventie is immers steeds de eerste stap !

Voor onder meer volgende preventieve diensten hebben wij sterke partners :

PEOPLE AWARENESS

INFRASTRUCTUUR AUDIT

NETWERK AUDIT

VEILIGE SOFTWARE

JURIDISCH ADVIES

Kempenlaan 29
2300 Turnhout

Doopput 14
2550 Kontich

www.cybercontract.eu
info@cybercontract.eu

Onafhankelijk tussenpersoon FSMA 113529A - RPR 0557.948.651 - BE02 0017 4242 4740

PEOPLE AWARENESS

Zijn uw mensen getraind op security awareness?

Iedere medewerker moet zich bewust zijn dat hij of zij op ieder moment kan gecontacteerd worden door iemand om informatie te ontfutselen. Iemand die plots belt met enkele onschuldig ogende vragen om meer informatie, een klusjesman die plots rondloopt, maar zelfs het correct gebruik van paswoorden zijn zaken waar men al het personeel dient op te trainen.

Hoe awareness verhogen?

Om awareness te verhogen bestaat er helaas geen gouden regel. Het is altijd bedrijfsspecifiek en dient te “passen” in de cultuur van het bedrijf. Soms kan dit door one-to-many training sessies, soms kan het aan de hand van computer-based training maar er zijn ook mogelijkheden als een kort bedrijfsfilmpje of andere creatieve mogelijkheden. Onze consultants passen al jaren diverse strategieën toe en kunnen deze perfect toespitsen op jullie cultuur.

Hoe kan je het testen?

Testen kan op diverse manieren, de meest gekende testen waarmee wij bedrijven assisteren, verlopen onder andere op volgende manieren:

- Versturen van phishingmails van diverse niveaus, gaande van overduidelijk phishing (denk aan de Koning van Namibië) tot zeer gerichte mails waarbij de werknemer in correct taalgebruik met zijn voornaam wordt aangesproken in een geloofwaardig scenario.
- USB drop-offs waarbij rapporten gemaakt worden om weer te geven hoeveel procent van de USB-sticks werd geconnecteerd met een PC, hoeveel procent van de mensen bestanden openden van de stick etc.
- Social engineering waarbij er specifieke doelen worden benaderd om te verifiëren of bedrijfspolicies rond het vrijgeven van specifieke informatie al dan niet gevolgd worden. Dit kan zowel telefonisch als in persoon gebeuren.

INFRASTRUCTUUR AUDIT

Data loss prevention: controle over je data

Wat kan de ontvanger doen met jou mail wanneer hij deze ontvangt? Wat als je medewerker al de data op een USB stick zet en doorverkoopt? Dat zijn vragen waar iedere bedrijfsleider van wakker ligt. Daarom dient ieder bedrijf data loss prevention technieken uitgewerkt te hebben waardoor het bijvoorbeeld niet langer mogelijk is om data te kopiëren of mails te printen of door te sturen. Hiervoor bestaan diverse oplossingen en kunnen wij assisteren in het maken van de juiste keuze en deployment.

Internal penetration test: de hacker van binnenuit

Wat indien iemand gewoon binnenwandelt en zijn laptop connecteert aan het netwerk, kan hij dan schade aanrichten? Kan hij diefstal van data plegen? Of die misnoegde werknemer, kan hij servers stoppen of virussen verspreiden? Het antwoord hierop dien je te kennen en niet te vrezen en daarom is het erg belangrijk een regelmatige controle te laten doen door een consultant met een hacker-mentaliteit die u kan uitleggen wat de te nemen acties zijn om de beveiliging op een hoog niveau te brengen.

Active Directory security health check

De Active Directory is vaak de database waarin alle gebruikers gedefinieerd staan maar is helaas ook vaak niet onder controle door jarenlange migraties van oude naar nieuwe versies of door slechte dagelijkse opvolging. Snel wordt het al eens vergeten dat een medewerker uit dienst gaat en behoudt hij alle rechten om in te loggen op afstand. Of vaak zijn er veel meer gebruikers administrator dan men vermoedt. Het is belangrijk om een test te doen om op basis van de uitkomst gerichte acties te nemen om het hart van de omgeving af te schermen voor misbruik.

CyberContract

Kempenlaan 29
2300 Turnhout

Doopput 14
2550 Kontich

www.cybercontract.eu
info@cybercontract.eu

Onafhankelijk tussenpersoon FSMA 113529A - RPR 0557.948.651 - BE02 0017 4242 4740

INFRASTRUCTUUR AUDIT

Virus uitbraak

Ook al staat op ieder toestel anti-virus geïnstalleerd, toch glipt regelmatig een virus door het mazen van het net en durft dan ernstig om zich heen te grijpen. Denk aan de recente uitbraken van ransomware waarbij data onleesbaar gemaakt wordt en een hacker geld vraagt om alles terug te zetten. Maar stopt het na 1 keer losgeld betalen? Na uitbraak van een virus is het extreem belangrijk om op de juiste mensen beroep te kunnen doen die samen met u het hoofd kunnen koel houden en snel de juiste beslissingen kunnen ondernemen.

Certificaten: hoe ze te gebruiken op een correcte manier

Voor talloze toepassingen worden certificaten gebruikt: voor het beveiligen van de website (https:// verbindingen) of het afschermen van gevoelige data intern. Helaas is de opzet vaak niet meer dan enkele ondoordachte klikken geweest waardoor men later in de problemen komt. Een doordacht design is van extreem belang en hier is ervaring de eerste vereiste.

NETWERK AUDIT

Controle van het design van je netwerk

Bij het ontwerpen van een nieuw netwerk of het herdefiniëren van een bestaand netwerk is het belangrijk dat dit samen met experten kan bekeken worden om zeker te zijn dat alle gekende valkuilen vermeden worden. Eens een nieuw netwerk in plaats is gebracht is het immers veel moeilijker om nog ingrijpende wijzingen aan te brengen.

Penetration testing vanaf de buitenkant: wie kan binnen?

Iedere minuut wordt een extern IP adres via het internet wel aangevallen door een van de talloze automatische scanners die bestaan maar ook in België vinden steeds meer en meer gerichte aanvallen plaats. Vaak proberen hackers via zwak beschermde firewalls binnen te dringen om dan zo verder te gaan naar de binnenkant van het bedrijf. Een externe controle is vaak beperkter vanwege het lage aantal beschikbare open poorten maar moet des te strikter gecontroleerd worden om het risico van een succesvolle aanval te minimaliseren.

Red team oefeningen: test mijn veiligheid

Steeds meer klanten willen weten wat mogelijk is in een realistisch aanvalsscenario: is het mogelijk om de boekhouding te bemachtigen? Is het mogelijk om onze klant informatie te stelen? En dit willen ze meten door een test te initiëren waarbij weinig tot geen informatie wordt vrijgegeven en de opdracht eruit bestaat om een aanval te lanceren zonder dat intern in het bedrijf veel mensen op de hoogte zijn. Op die manier kan niet alleen gekeken worden hoe moeilijk het is om binnen te geraken maar ook de reacties kunnen getest worden indien interne IT ziet dat bepaalde zaken plaatsvinden en zij langzaam controle verliezen.

CyberContract

Kempenlaan 29
2300 Turnhout

Doopput 14
2550 Kontich

www.cybercontract.eu
info@cybercontract.eu

VEILIGE SOFTWARE

Begin er al aan tijdens een project, niet na een project

Het ontwikkelen van veilige software doe je vanaf de start. Omdat veiligheid in software iets zeer specifiek is dien je dit niet zelf te doen maar op tijd een expert te betrekken. Deze expert hoeft zelfs niet continu bij het project betrokken te zijn maar kan bijvoorbeeld 1 keer per week samenkomen met de stakeholders van het project om de specifieke vragen rond security te behandelen. Deze expert kan je begeleiden in het nemen van de juiste beslissingen en kan op een meest opportune manier de penetration testen voor de software inplannen zodat er wordt gewerkt met een oog op kwaliteit en kosten-efficiëntie.

Ontwikkelaars? Train ze!

Het merendeel van de ontwikkelaars kent wel enkele veiligheidsrisico's maar helaas worden ze er dermate weinig mee geconfronteerd dat het in de praktijk wel eens vergeten wordt. Het is van extreem belang dat ontwikkelaars een training volgen waarbij ze zelf de kans krijgen om enkele voorbeeld applicaties of hun eigen applicaties eens aan te vallen. Door het zelf te doen beseffen ze niet alleen dat een hacker het niet altijd moeilijk heeft maar worden ze zich veel bewuster van het risico waardoor ze in de toekomst veel meer aware gaan zijn en tijdig hulp zullen inroepen.

Penetration testing op applicaties

In deze tijd is het niet meer verantwoord om nog applicaties te publiceren op het interne of externe netwerk zonder ze eerst te onderwerpen aan een penetration test. Het belang hievan is niet te onderschatten gezien hackers steeds op een publieke manier een bedrijf zullen schaden door bekend te maken dat bijvoorbeeld een database gestolen werd of door hen af te persen en geld te vragen om de buitgemaakte data niet te publiceren. Jaarlijks dient gecontroleerd te worden of er geen nieuwe exploits gekend zijn die misbruikt kunnen worden om de applicatie aan te vallen en of er geen code werd toegevoegd die fouten bevat waardoor de applicatie een verhoogd risico loopt.

CyberContract

Kempenlaan 29
2300 Turnhout

Doopput 14
2550 Kontich

www.cybercontract.eu
info@cybercontract.eu