Mystery Guest

MBO Digitaal

Samenwerken aan cyberveiligheid

11 december 2025

CYBER SEALS

seal the gaps & secure the future

Agenda

- VOORSTELLEN
- OVER CYBER SEALS
- NIEUWS
- MYSTERY GUEST
- AANPAK (en praktijk voorbeelden)
- LESSEN UIT DE PILOTS
- TIPS & CTA
- VRAGEN

CYBER SEALS

voorstellen

Jelle Mulckhuijse

Directeur & Ethisch Hacker

CYBER SEALS

voorstellen

Richard Hulzinga

Chief of Operations & Security Adviseur

voorstellen

Joris Cras

Ethical Hacker & Cybersecurity Specialist

Overzicht diensten

40
specialisten

Vulnerability scan
Geautomatiseerd onderzoek naar bekende kwetsbaarheden binnen systemen en netwerken voor tijdige risico-identificatie.

Phishing
Simulatie van phishing-aanvallen om bewustzijn, gedrag en respons van medewerkers te beoordelen.

Trainingen
Professionele cybersecuritytrainingen gericht op kennisvergroting, bewustzijn en gedragsverandering.

Cybersecurity advisory
Strategisch advies voor risicobeheersing, beleidsontwikkeling en cyberweerbaarheid

Pentest
Diepgaande handmatige test waarbij ethisch hackers kwetsbaarheden onder realistische omstandigheden identificeren.

Red teaming
Integrale aanvalssimulatie waarmee weerbaarheid van systemen, processen en mensen wordt getest.

IAM
Inrichting en optimalisatie van toegangsbeheer om gebruikersrechten veilig en gecontroleerd te beheren.

Compliance
Begeleiding bij implementatie en naleving van informatiebeveiligingsnormen en regelgeving.

USB-dropping
Beveiligingsonderzoek via geplaatste USB-sticks om fysieke security awareness te meten.

Hack demo
Live demonstratie van hacktechnieken om inzicht te geven in actuele digitale dreigingen.

Privacy
Advies en ondersteuning bij naleving van privacywetgeving en bescherming van persoonsgegevens.

Supplier security
Beoordeling en beheersing van beveiligingsrisico's binnen de keten van externe leveranciers.

Mystery Guest
Fysieke beveiligingstoetsing door gecontroleerde toegangspogingen op locatie door een anonieme specialist.

Secure development
Begeleiding bij integratie van beveiligingsprincipes binnen de softwareontwikkelingscyclus.

SOC/SIEM
Onze SOC-experts optimaliseren jouw SOC met use cases, SIEM-advies en volwassenheidsanalyses.

Risk management
Systematische identificatie, beoordeling en beheersing van informatiebeveiligingsrisico's binnen de organisatie.

In het nieuws

> Bad news travles at the speed of light; good news travels like molasses.

28 okt 2024 om 12:27
Update: 1 week geleden

111 reacties | Delen

Rusland en China voeren hun cyberaanvallen op Nederland en zijn bondgenoten op, waarschuwt de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Staring College betaalt losgeld na grote cyberaanval

26 februari 2021, 19:11 • 2 minuten leestijd

Het Staring College werd getroffen door een cyberaanval.
© ANP

LOCHEM - Het Staring College is deze week getroffen door een grote cyberaanval. De middelbare school uit Lochem en Borculo heeft losgeld

Onderwijsstichting OSG Hengelo slachtoffer van hack: servers versleuteld na aanval met gijzelsoftware

2 juni 2023, 14:19 • Aangepast 3 juni 2023, 19:49 • 2 minuten leestijd

NOS Nieuws • Donderdag 16 januari 2025, 11:31 •
Aangepast donderdag 16 januari 2025, 14:59

Internet op onderwijsinstellingen ontregeld door ddos-aanval

Verschillende onderwijsinstellingen hebben te maken met trage of geen internetverbinding door een ddos-aanval, dat laat netwerkbedrijf SURF weten. Meerdere onderwijs- en onderzoeksinstellingen door het land ondervinden problemen omdat ze via SURF een gemeenschappelijk ICT-netwerk delen.

De universiteit van Maastricht laat desgevraagd weten vanochtend drie kwartier zonder internetverbinding te hebben gezeten. Ook het Máxima MC Eindhoven

Tienduizenden verkeerslichten in Nederland te hacken, lek nog jaren te misbruiken

Door Daniël Verlaan · 5 oktober 2024 · Aangepast: 25 oktober 2024

Mystery Guest

- Iemand die zich voordoet als iemand anders.
- Focus op de menselijke factor.
- Toetsen toegangscontroles, beveiligingsprocedures.

Doel:

Het doel is om kwetsbaarheden in het dagelijkse beveiligingsgedrag van medewerkers en processen op te sporen en te verbeteren, en zo de cyberbeveiliging van de organisatie te versterken.

Mystery Guest als praktijk aanvulling op de E-learning.

Aanpak

Stappenplan Mystery Guest

1

Vooronderzoek

- Analyseren van openbare bronnen zoals website, social media en Google Maps.
- In kaart brengen van personeel, gebouwindeling en dagelijkse routines.
- Identificeren van mogelijke zwakke plekken en risicomomenten.
- Observatie op locatie (meestal 2 keer) zonder herkenning.
- Vaststellen van uitvoerbaarheid en kansen voor scenario's.

2

Scenario ontwikkelen en voorbereiding

- Uitwerken van één of meerdere realistische aanvalsscenario's.
- Bepalen van doelen, stappen, middelen en omgaan met onverwachte situaties.
- Rollen zoals ouder, leverancier of student worden geloofwaardig ingevuld.
- Voorbereiden van kleding, ID's en technische hulpmiddelen (zoals USB of mini-pc).
- Grondige voorbereiding voor maximale slagingskans en minimale risico's.

3

Uitvoering

- Mystery Guest voert de actie uit volgens het gekozen scenario.
- Gericht op toegang tot risicovolle plekken zoals server- of administratieruimtes.
- Observatie van medewerkersreacties en onbeveiligde informatie of systemen.
- Indien nodig wordt een tweede poging gedaan met alternatief scenario.
- Alles gebeurt discreet, zorgvuldig gedocumenteerd en binnen afgesproken kaders.

4

Rapportage

- Uitgebreid rapport met stappen, scenario's, risico's en medewerkersreacties.
- Inclusief praktische en haalbare verbeteradviezen voor de praktijk.
- Rapport ondersteunt bewustwording én beleidsaanpassing.
- Optioneel: anonieme videocompilatie ter ondersteuning van presentaties.
- Betrouwbare en representatieve resultaten dankzij zorgvuldige aanpak.

Lessen uit de 4 pilots

- Medewerkers zijn vaak erg behulpzaam en spreken onbekenden niet snel aan (beveiliging wordt vaak als vriendelijkheidsdilemma ervaren).
- Procedures bestaan wel, maar worden onvoldoende/niet nageleefd.
- Standaard sloten serverkasten.

Praktische tips voor medewerkers

1. Spreek onbekenden vriendelijk maar direct aan.
2. Maak het normaal om vragen te stellen: cultuur van veiligheid.
3. Gebruik korte vragen: “Kan ik u ergens mee helpen?”
4. Houd je aan procedures, ze bestaan met een reden.
5. Oefen met realistische scenario’s om alertheid te vergroten.

Afsluiting en call to action

- Bewustzijn en gedrag zijn de kern van fysieke beveiliging.
- Procedures werken pas als mensen ze toepassen.
- Mystery guest-tests tonen realistische risico’s én verbeterkansen.
- Samen bouwen aan een cultuur van alertheid en aanspreken.
- Volgende stap: structureel testen, trainen en verbeteren…

!

Start vandaag nog

CYBER SEALS

Cyber Seals B.V.

Tractieweg 41, Studio E
3534 AP
Utrecht

+31(0)85 40 16 032

info@cyberseals.nl

cyberseals.nl

KvK: 76058247
BTW-nr.: NL860492679B01

Richard Hulzinga

E: richard@cyberseals.nl
M: 06 276 111 89