Publicatiedatum : 03/01/2024

Opleiding : Ransomware, inzicht in de bedreiging

Aanvallen voorkomen en incidenten verhelpen

seminarie - 2d - 14u00 - Ref. RAN

Prijs : 1850 € V.B.

Nouvelle édition

Er gaat bijna geen dag voorbij zonder dat de media ons waarschuwen voor een nieuwe ransomware-aanval op een ziekenhuis, gemeente of bedrijf. Tussen januari 2022 en juni 2023 heeft het ANSSI alleen al 187 cyberaanvallen op lokale overheden afgehandeld. In slechts een paar jaar tijd is ransomware uitgegroeid tot de grootste plaag van cybercriminaliteit ter wereld. Deze cursus helpt je de mechanismen achter ransomware-aanvallen te begrijpen. U leert ook hoe u zich ertegen kunt beschermen en hoe u een dergelijke crisis het beste kunt beheersen.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- Inzicht in de ransomware-bedreiging en hoe cybercriminelen te werk gaan
- Ontdek het ecosysteem van ransomware (RaaS, filialen, IAB, enz.)
- De belangrijkste beveiligingsmaatregelen identificeren om hiertegen te beschermen
- Leer meer over best practices om de cyberweerbaarheid van uw bedrijf te garanderen
- Een grootschalige cybercrisis beheren in verband met een ransomware-aanval

Doelgroep

CISO's, IT-directeuren, architecten, ontwikkelaars, projectmanagers, pre-sales vertegenwoordigers, systeem- en netwerkbeheerders.

Voorafgaande vereisten

Algemene computerkennis is aanbevolen.

Opleidingsprogramma

DEELNEMERS

CISO's, IT-directeuren, architecten, ontwikkelaars, projectmanagers, pre-sales vertegenwoordigers, systeem- en netwerkbeheerders.

VOORAFGAANDE VEREISTEN

Algemene computerkennis is aanbevolen.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

1 De ransomware-bedreiging begrijpen

- De belangrijkste ransomwareprogramma's en hoe ze zijn geëvolueerd sinds AIDS/PC Cyborg (1989) tot nu.
- Evolutie van de dreiging: van eenvoudige tot viervoudige afpersing.
- Typologie van getroffen bedrijven.
- De 10 mythes van ransomware.
- De motivaties van cybercriminelen (geld is niet altijd het doel...).
- Wie zijn de belangrijkste groepen cybercriminelen die gespecialiseerd zijn op dit gebied?
- Het cybercriminele ecosysteem (RaaS-groep, filialen, IAB, BPHS, dark web).
- Anonimiteit en de modus operandi van cybercriminelen.
- Het Ransomware as a Service (RaaS) bedrijfsmodel.
- Veranderingen in het aantal aanvallen in de afgelopen 3 jaar.

2 Impact van cyberaanvallen op bedrijven

- Wat zijn de directe en indirecte kosten van een cyberaanval?
- Wat is het gemiddelde/mediane losgeldbedrag? Hoe wordt het berekend?
- Is het mogelijk om te onderhandelen? Welke speelruimte is er? Andere voordelen van onderhandelen.
- Moet er losgeld worden betaald? Is het ANSSI-standpunt nog steeds van toepassing?
- Hoe kun je gegevens herstellen na betaling?
- Het debat in Frankrijk over verzekeraars die losgeld betalen en de LOPMI 2023.

3 Juridische aspecten

- De belangrijkste Franse wetten over cybercriminaliteit en cyberbeveiliging.
- Wettelijke verplichtingen op het gebied van gegevensbescherming.
- Wat zijn de straffen voor cybercriminelen?
- De gerechtelijke behandeling van cybercriminaliteit in Frankrijk, Europa en de rest van de wereld.
- Hoe de wereldwijde strijd tegen cybercriminaliteit is georganiseerd: het Verdrag van Boedapest en MLAT.
- Hoe effectief zijn onderzoeken en vervolgingen buiten Frankrijk?

Workshop storytelling

Voorbeelden van gearresteerde cybercriminelen.

4 Anatomie van een moderne ransomware-aanval

- Beschrijving van een "Jacht op groot wild" aanval.
- De kill chain: van eerste toegang tot afpersing.
- Analyse van de gebruikte tactieken, technieken en procedures (TTP) met behulp van het MITRE ATT&CK-raamwerk.
- De spraakmakende WannaCry en NotPetya cyberaanvallen.
- Aanvallen op OIV (Colonial Pipeline), leverancier (Kaseya) of ziekenhuis (CHSF Corbeil-Essonnes).

Workshop storytelling

Enkele beroemde cyberaanvallen en feedback.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

5 Eerste toegang tot het informatiesysteem

- Identificeer het aanvalsoppervlak van uw bedrijf.
- De 9 technieken die worden gebruikt om initiële toegang te krijgen.
- Social engineering-aanvallen (spear phishing, deepfake phishing, enz.).
- Problemen met toegang op afstand (RDP en VPN).
- De belangrijkste softwarekwetsbaarheden die door ransomware worden uitgebuit (CVE, CVSS en EPSS).
- Aanvallen via de toeleveringsketen.

6 De belangrijkste beveiligingsoplossingen identificeren

- Waarom en hoe gebruikers bewust maken?
- Hoe EPP-oplossingen zich verhouden tot traditionele antimalware.
- Inzicht in de rol en complementariteit van EPP-, EDR-, NDR- en XDR-oplossingen.
- De beveiliging van Active Directory (AD) versterken.
- Netwerksegmentatie en de toepassing van het Zero Trust principe op AD en back-ups.
- Scannen op kwetsbaarheden en patchbeheer.
- Risicobeheer van ransomware via de toeleveringsketen.
- Wat zijn de meest effectieve beveiligingsmaatregelen?
- Evaluatie van het ROM (verhouding tussen effectiviteit en gebruiksgemak) van de belangrijkste beveiligingsoplossingen.

7 De cyberweerbaarheid van uw bedrijf garanderen

- Voer een specifieke bedrijfsimpactanalyse uit voor de ransomware-dreiging.
- Bedrijfscontinuïteitsplannen (BCP) en rampenherstelplannen (DRP).
- Waarom is de 3-2-1 vrijwaringsregel niet langer voldoende?
- Veilige back-ups (versleuteling, onveranderlijkheid, offline modus).
- Cyberverzekeringscontracten (garanties, kosten, uitsluitingen en limieten).

8 Een ransomwarecrisis beheren

- Organisatie van de crisiseenheid.
- De belangrijkste fasen in een ransomwarecrisis.
- Interne en externe communicatie: welke mate van transparantie?
- Geheimhouding van het onderzoek en toepassing van artikel 11 van de CPP.
- De belangrijkste fouten die u moet vermijden bij het beheren van een ransomwarecrisis.
- Crisisafsluiting en Retex.

Data en plaats

KLAS OP AFSTAND
2026 : 2 juni, 17 sep., 3 dec.

PARIS LA DÉFENSE
2026 : 26 mei, 10 sep., 26 nov.