Ransomware, comprendre la menace
Prévenir les attaques et remédier aux incidents

Séminaire de 2 jours - 14h
Réf : RAN - Prix 2024 : 2 090CHF HT

Il ne se passe plus un seul jour sans que les médias nous alertent d'une nouvelle attaque par rançongiciel sur un hôpital, une collectivité locale ou une entreprise. L'ANSSI a traité 187 cyberattaques sur la seule cible des collectivités territoriales entre janvier 2022 et juin 2023. Le ransomware est devenu, en quelques années, le fléau cybercriminel n°1 dans le monde. Cette formation vous permettra de saisir les mécanismes des attaques par ransomwares. Vous verrez également comment vous en prémunir et gérer au mieux une crise de ce type.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre la menace ransomware et le mode opératoire des cybercriminels

Découvrir l'écosystème du ransomware (RaaS, affiliés, IAB…)

Identifier les principales mesures de sécurité pour s'en prémunir

Connaître les bonnes pratiques pour assurer la cyberrésilience de son entreprise

Gérer une crise cyber de grande ampleur liée à une attaque par ransomware

LE PROGRAMME

dernière mise à jour : 01/2024

1) Comprendre la menace ransomware

- Les principaux rançongiciels et leur évolution depuis AIDS/PC Cyborg (1989) à aujourd'hui.
- Évolution de la menace : de la simple à la quadruple extorsion.
- Typologie des entreprises impactées.
- Les 10 mythes du ransomware.
- Les motivations des cybercriminels (l'argent n'est pas toujours le but…).
- Qui sont les grands groupes de cybercriminels spécialisés dans ce domaine ?
- L'écosystème cybercriminel (Groupe RaaS, affiliés, IAB, BPHS, dark web).
- Anonymat et modus operandi des cybercriminels.
- Le modèle économique du Ransomware as a Service (RaaS).
- L'évolution du nombre d'attaques ces 3 dernières années.

2) Impact des cyberattaques pour les entreprises

- Quels sont les coûts directs et indirects d'une cyberattaque ?
- Quel est le montant moyen/médian des rançons ? Comment est-il calculé ?
- Peut-on négocier ? Quelle est la marge de manœuvre ? Autres intérêts d'une négociation.
- Faut-il payer les rançons ? La position de l'ANSSI est-elle toujours applicable ?
- Comment se passe la récupération des données après paiement ?
- Le débat en France autour de la prise en charge des rançons par les assureurs et la LOPMI 2023.

3) Aspects juridiques

- Les principales lois françaises en matière de cybercriminalité et de cybersécurité.

PARTICIPANTS

RSSI, DSI, architectes, développeurs, chefs de projet, commerciaux avant-vente, administrateurs système et réseau.

PRÉREQUIS

Des connaissances générales sur l'informatique sont recommandées.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Les obligations réglementaires en matière de protection des données.
- Quelles sont les sanctions encourues par les cybercriminels ?
- Le traitement judiciaire de la cybercriminalité en France, en Europe et dans le monde.
- Comment s'organise la lutte mondiale contre la cybercriminalité : convention de Budapest et MLAT.
- Quel est l'efficacité des investigations et des poursuites judiciaires en dehors de l'Hexagone ?

Echanges : Exemples d'arrestations de cybercriminels.

4) Anatomie d'une attaque moderne par rançongiciel

- Description d'une attaque de type "Big Game Hunting".
- Déroulement de la kill chain : de l'accès initial à l'extorsion.
- Analyse des tactiques, techniques et procédures utilisées (TTP) avec le framework MITRE ATT&CK.
- Les cyberattaques médiatisées WannaCry et NotPetya.
- Attaques sur OIV (Colonial Pipeline), fournisseur (Kaseya) ou hôpital (CHSF Corbeil-Essonnes).

Echanges : Quelques cyberattaques célèbres et retours d'expérience.

5) L'accès initial au système d'information

- Identifier la surface d'attaque de son entreprise.
- Les 9 techniques utilisées pour obtenir un accès initial.
- Les attaques par ingénierie sociale (spear phishing, deepfake phishing…).
- La problématique des accès distants (RDP et VPN).
- Les principales vulnérabilités logicielles exploitées par les rançongiciels (CVE, CVSS et EPSS).
- Les attaques via la chaine d'approvisionnement (supply chain).

6) Identifier les principales solutions de sécurité

- Pourquoi et comment sensibiliser les utilisateurs ?
- L'apport des solutions EPP par rapport aux antimalwares traditionnels.
- Comprendre le rôle et la complémentarité des solutions EPP, EDR, NDR et XDR.
- Le renforcement de la sécurité d'Active Directory (AD).
- La segmentation des réseaux et l'application du principe de Zero Trust sur AD et les sauvegardes.
- Le scanning des vulnérabilités et la gestion des correctifs de sécurité.
- La gestion du risque ransomware via la supply chain.
- Quelles sont les mesures de sécurité les plus efficaces ?
- Évaluation du ROM (ratio efficacité/facilité d'exploitation) des principales solutions de sécurité.

7) Assurer la cyberrésilience de son entreprise

- Réaliser un Business Impact Analysis spécifique à la menace ransomware.
- Les plans de continuité (PCA) et de reprise d'activité (PRA).
- Pourquoi la règle de sauvegarde 3-2-1 n'est-elle plus suffisante ?
- La sécurisation des backups (chiffrement, immuabilité, mode offline).
- Les contrats de cyberassurance (garanties, coûts, exclusions et limites).

8) Gestion d'une crise ransomware

- Organisation de la cellule de crise.
- Les principales étapes d'une crise ransomware.
- Communication interne et externe : quel niveau de transparence ?
- Le secret de l'enquête et application de l'article 11 du CPP.
- Les principales erreurs à éviter dans la gestion d'une crise ransomware.
- Clôture de crise et Retex.

LES DATES

CLASSE À DISTANCE
2024 : 20 juin, 09 sept., 25 nov.