
AUDIT CYBERSECURITE
L'incontournable 360 de votre cybersécurité pour une meilleure protection de votre système d'information.
FRANCE RELANCE
EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE
[N]
FRANCE NUM

Contexte et Objectifs

Contexte

L'année 2021 a vu l'explosion et la médiatisation des cyberattaques.

La menace cyber exploite avec efficacité certaines vulnérabilités inhérentes à la transformation numérique de la société et de l'économie. Le télétravail ainsi que la crise du Covid ont transformé nos usages ouvrant ainsi la porte à de nouvelles attaques ciblant les TPE – PME.

Les acteurs privés et publics sont ciblés, 77% des victimes d'attaques sont des PME.
Les formes les plus répandues sont :
- Les rançongiciels
- La fraude aux virements
- Les vols de données et déni de service
- Les tentatives de fraudes et d'usurpation d'identité
- Les défigurations de sites internet professionnels

Objectifs

Nous accompagnons nos clients dans leur transformation numérique pour une expérience simple, respectueuse et sécurisée.

Choisir Cyberzen assure un service de haut niveau, ancré dans le présent et résolument tourné vers l'avenir. Nous souhaitons simplifier l'usage de l'outil informatique et de la cybersécurité pour vous aider à vous focaliser sur vos véritables enjeux : votre cœur de métier et vos clients.

Pour cela, nous vous accompagnons de bout en bout en commençant par l'audit et le conseil jusqu'au développement de solutions métiers dédiées.
Choisir Cyberzen, c'est s'assurer des services reconnus et récompensés, bénéficier de plus de vingt ans d'expérience dans ces domaines et aborder l'avenir de manière sereine.

Nos services

Audits

- D'hygiène cyber, fonctionnel et / ou organisationnel
- De fournisseurs
- D'hygiène cyber pré-acquisition (due diligence)
- De code source
- D'Active Directory
- De vulnérabilité (scans)

Pentests

- Red Team ou Purple Team
- White Box
- Grey Box
- Black Box

Formation

- Conférences de sensibilisation
- Serious Game VR / Web / mobile
- Coaching

Transformation Numérique

- Développement d'applications métier
- Conseils IT & Cybersécurité
- DSI / RSSI Temps Partagé

L’audit de CYBERZEN

L’Agence Nationale de la Sécurité de Systèmes d’Information (ANSSI) a publié un guide d’hygiène pour la cybersécurité. Ce guide a pour but d’établir règles d’hygiène informatique les plus simples et élémentaires, transposition dans le monde numérique de règles de sécurité sanitaire.

CYBERZEN a développé une méthodologie d’audit primée « Prix de la démarche la plus innovante » aux assises de la cyber sécurité.
Cet audit vous donne une vue globale sur la maturité en cybersécurité.
Vous trouverez dans le rapport qui vous est fourni un résumé de la méthodologie ainsi qu’un plan de remédiation pragmatique qui vous indique pour chaque élément un coût de mise en place, la difficulté relative pour y arriver et l’amélioration que cela apporte pour votre système d’information.

Guide d'hygiène *ANSSI*

L'ANSSI a publié un guide d'hygiène pour la cybersécurité[1]. Ce guide a pour but d'établir règles d'hygiène informatique les plus simples et élémentaires, transposition dans le monde numérique de règles de sécurité sanitaire.

À mesure des années, ce guide s'est imposé comme l'état de l'art indiscutable pour toutes les structures au point d'être intégré dans tous les référentiels (SecNumCloud, NIS2, DORA…) comme la base ne pouvant être négociée.

C'est pourquoi nous vous proposons des packs qui vous permettent d'aligner votre cybersécurité avec l'état de l'art.

cyberzen

AUDIT une vue 360 de votre SI

Les thèmes expliqués (1)

Sensibiliser et former

Les menaces évoluent tous les jours. Sans la participation des usagers du système d'information, il est vain d'espérer pouvoir contrer les menaces et les attaques. C'est pour cela qu'il est important que chaque utilisateur puisse recevoir régulièrement une sensibilisation à ce sujet. Par ailleurs, les administrateurs informatiques ayant un grand pouvoir, il est primordial qu'ils soient à jour techniquement.

Connaître le système d'information

Comment se protéger lorsque l'on ne sait pas ce que l'on doit protéger ? C'est sous cet angle simple qu'on nous préconise de récolter des informations autour du réseau, des données sensibles ou encore des droits d'accès des utilisateurs.

Sécuriser l'administration

Un grand pouvoir impliquant de grandes responsabilités, l'ANSSI recommande la séparation des réseaux d'utilisation et d'administration, ainsi qu'une vigilance particulière de ceux-ci.

Les thèmes expliqués (2)

Authentifier et contrôler les accès

Les accès sont les portes d'entrée du système d'information, ils doivent être minutieusement contrôlés pour s'assurer qu'aucune personne non autorisée n'y pénètre. On s'intéressera donc aux technologies d'authentification, aux droits des administrateurs et des utilisateurs.

Sécuriser les postes

Le poste de travail est à l'utilisateur ce qu'est le marteau à celui qui veut planter un clou : un outil indispensable. Tellement indispensable que lorsqu'il n'est plus disponible, on se retrouve au chômage technique. Afin que cela n'arrive pas, il faut veiller à appliquer des règles d'hygiène simples.

Sécuriser le réseau

Le réseau est l'ossature du système d'information. Il requiert un soin particulier lors de sa construction et de la mise en place des briques technologiques qui le constituent car elles apporteront fonctionnalités et sécurité. Tout comme les postes de travail, les équipements qui constituent le réseau s'entretiennent. Les technologies évoluant, un soin constant doit être apporté à leur égard.

cyberzen

Les thèmes expliqués (3)

Gérer le nomadisme

Avec l'arrivée généralisée des smartphones et de la 4G, la station de travail n'est plus statique. On la retrouve dans le train, l'avion, en rendez-vous client, à l'étranger... Cette avancée pour l'utilisateur induit une contrainte de sécurité. En effet, tous ces accès sont des portes d'entrée vers l'entreprise.

Maintenir à jour le système d'information

Le système d'information est vivant. Il évolue, reçoit des données, en distribue, fait face à des usages qui le font muter. Pour une bonne santé, il faut donc le maintenir et s'assurer que son hygiène quotidienne est à l'état de l'art.

Superviser, auditer, réagir

En cas d'incident, il est toujours plus simple d'avoir anticipé. En effet, chercher une aiguille dans une botte de foin est fastidieux, surtout lorsqu'elle n'existe pas. Autrement dit, il faut commencer par superviser, puis auditer régulièrement son système d'information afin de pouvoir réagir en cas d'attaque.

cyberzen

LES PLUS-VALUES DE L'AUDIT

Rassurer vos partenaires

Notre audit peut répondre aux exigences de conformité de cybersécurité de vos partenaires.

Notre outil permet de répondre aux attentes des assureurs, tant sur les points techniques que documentaires.

Débuter à documenter

Remédiation maitrisée

Notre plan de remédiation vous donne un plan d'action avec les projections des coûts et du planning.

Sensibilisation

Vos employés sont cruciaux dans la mise en place d'une politique de cybersécurité réussie.

COMMENT SE PASSE NOTRE AUDIT?

Analyse

de la documentation reçue

Evaluation

par notre expert

Réunion

préliminaire. Envoi de la liste documentaire

Interviews

des responsables fonctionnels (internes et externes si besoin)

Restitution

Réunion avec le client et présentation du plan d'action

Points pratiques

L’audit ne demande pas d’arrêter de votre système informatique.

L’audit ne met pas à risque votre système d’information.

L’audit couvre un large scope sur les domaines de la gouvernance, de l’organisation, du fonctionnel et du technique.

Les audits sont menés par nos experts séniors.