everping

Guide

Le guide de la sécurité informatique

Les 10 couches de défense à mettre en place et le rôle de chacune.

Les PME et les ETI sont la cible idéale : assez de données et de trésorerie pour qu'une attaque soit rentable, rarement assez de moyens pour se défendre comme un grand groupe. La bonne nouvelle : l'essentiel du risque se couvre avec une poignée de fondamentaux bien posés.

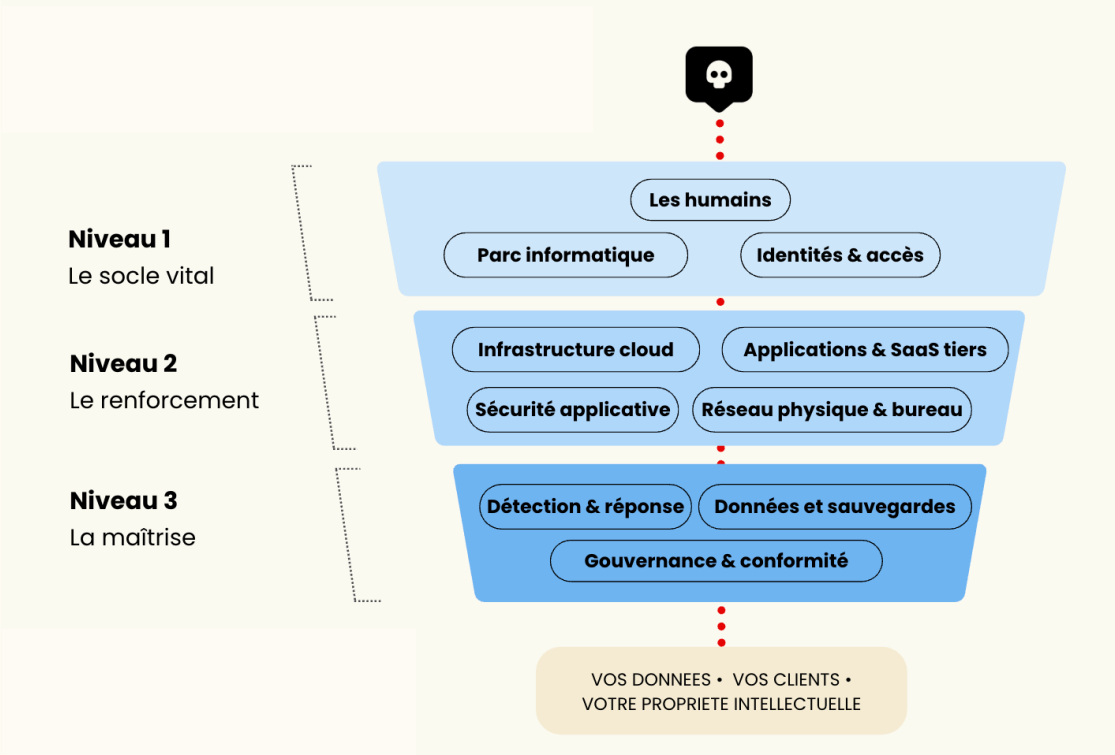
Ce guide ne vous donne pas une liste de tâches à cocher. Il cartographie le terrain de façon synthétique et explique, couche par couche, contre quoi chacune vous protège — pour que vous puissiez arbitrer en connaissance de cause.

Un principe clé à garder en tête : aucune mesure n'est suffisante seule. On empile des couches indépendantes pour qu'une faille — un mot de passe volé, un ordinateur perdu, un email piégé — n'ouvre jamais l'accès direct à vos données.

Aurélien Negret
CEO d'Everping

Les couches de défenses

La sécurité informatique ne repose pas sur un outil unique, mais sur l'empilement de 10 couches de défense, classées en 3 niveaux. Chacune protège contre des menaces différentes; c'est leur superposition qui fait qu'une faille isolée ne suffit jamais à atteindre vos données.



Niveau 1 - Le socle vital

Les surfaces qui couvrent les attaques les plus fréquentes et qui ne dépendent de rien d'autre pour être efficaces. Vitales dès le jour 1, même pour une structure qui ne fait que de la bureautique. La question qu'elles adressent :

> « Qu'est-ce qui, si ce n'est pas fait, peut couler l'entreprise avec une attaque banale ? »

Ces 3 premières couches couvrent l'écrasante majorité des incidents réels. Tant qu'elles ne sont pas solides, investir ailleurs revient à blinder la porte en laissant la fenêtre ouverte.

Niveau 2 - Le renforcement

Ce sont les couches qu'on solidifie une fois le socle posé, parce qu'elles le présupposent et parce qu'elles grandissent avec l'entreprise. La question :

> « qu'est-ce qui réduit la surface invisible qui s'étend à mesure qu'on grossit ? »

Une fois le socle en place, on réduit la surface invisible : le SaaS qui prolifère et l'infrastructure qui s'ouvre à mesure que l'entreprise grandit.

Niveau 3 - La maîtrise

C'est le passage de « on se protège » à « on pilote, on maîtrise et on prouve ». La question :

> « qu'est-ce qui nous fait passer de subir à maîtriser ? »

À noter

Ce n’est pas une vérité universelle à 100% : une entreprise qui vient de subir une cyberattaque a besoin de rémédiation tout de suite. Une startup régulée (finance, cybersécurité) a besoin d’un produit sécurisé dès le 1er jour. Mais dans la majorité des cas, c’est le bon ordre.

everping

Guide

Les couches de défense, une par une

Pour chaque couche : ce qu'elle est, contre quoi elle protège, et ce qu'elle recouvre concrètement. Classées du socle vital vers le pilotage maîtrisé.

Niveau 1 - Le socle vital

01 - Les humains

→ Former et sensibiliser vos collaborateurs

Rôle

Vos collaborateurs sont la première surface d'attaque. La majorité des intrusions commencent par un email piégé, un appel d'ingénierie sociale ou une simple erreur — pas par une prouesse technique.

Leviers

Sensibilisation continue, simulations de phishing, culture du signalement, vigilance sur les fraudes au virement et à l'usurpation de dirigeant.

02 - Parc informatique

→ Protéger l'ensemble des ordinateurs de l'entreprise et savoir exactement ce que chacun possède.

Rôle

Chaque ordinateur manipule vos données et est une porte d'entrée dans le reste du système. Même si vous êtes 100% cloud, un poste compromis - ou un ordinateur perdu qui n'est pas chiffré — c'est une fuite directe.

Leviers

Déploiement d'un MDM sur chaque ordinateur (inventaire, verrouillage et effacement à distance, forcer les configurations de sécurité), EDR au-delà de l'antivirus classique, gestion des mises à jour, encadrement du BYOD, effacement en fin de vie.

03 - Identités & accès

→ La gestion de qui peut se connecter à quel outil et comment

Rôle

un seul mot de passe volée ou oublié peut ouvrir toutes vos applications et vos systèmes. Protéger les identités et les accès, c'est empêcher qu'un seul identifiant volé n'ouvre tout et assurer que tous les comptes n'ont pas tous les droits.

Leviers

MFA obligatoire sur 100 % des comptes, SSO sur un maximum d'applications, un gestionnaire de mots de passe d'entreprise, et un process d'offboarding rigoureux.

Niveau 2 - Le renforcement

04 - Infrastructure cloud

→ Votre infrastructure cloud où tournent vos produits et vos données (serveurs, base de données, réseau cloud)

Rôle

Tout y dépend de votre configuration : un stockage laissé public ou un accès trop large suffit à transformer une petite faille en compromission générale.

Leviers

Durcissement des consoles cloud avec MFA, IAM cloud et moindre privilège sur les rôles et les comptes de service, réseau cloud (VPC, subnets privés, security groups), segmentation des services, et gestion propre des secrets.

05 - Sécurité applicative

→ La sécurité des logiciels que vous construisez vous-même, du code jusqu'à sa mise en production

Rôle

Empêcher qu'une faille dans votre propre produit — ou dans sa chaîne de fabrication — ne devienne le point d'entrée.

Leviers

Secure coding et revue de code, scan des dépendances open-source (supply chain logicielle), zéro secret dans les dépôts Git, sécurisation de la chaîne CI/CD, prise en compte de l'OWASP Top 10, et scan de vulnérabilités régulier ainsi que tests d'intrusion (pentest) pour valider l'ensemble avant les attaquants.

06 - Réseau physique & bureau

→ La connectivité et les accès de vos locaux : réseau filaire, WiFi, et accès physique aux lieux et au matériel.

Rôle

Empêcher qu'un point d'entrée local — une borne WiFi, une prise réseau, une porte non contrôlée — ne serve de tremplin vers le système d'information.

Leviers

WiFi sécurisé et réseau invité totalement étanche, segmentation, contrôle des accès au bâtiment et aux salles techniques, infra locale.

07 - Applications & SaaS tiers

→ Reprendre le contrôle sur les dizaines/centaines d'outils que vos équipes consomment au quotidien — CRM, messagerie, gestion de projet, RH, paie…

Rôle

Vos données vivent chez des éditeurs tiers, accessibles par simple identifiant depuis tout Internet. Le vrai risque, c'est leur prolifération : chaque outil est une porte vers vos données, et chaque porte que vous ne connaissez pas est une porte que vous ne pouvez pas fermer.

Leviers

Inventaire des SaaS, maîtrise du Shadow IT, revues d'accès et moindre privilège dans chaque application, contrôle des intégrations OAuth, sécurité de la messagerie (DMARC, SPF, DKIM).

Niveau 3 - La maîtrise

08 - Détection & réponse

→ La capacité à voir ce qui se passe et à réagir vite quand une attaque réussit malgré tout.

Rôle

Réduire le temps entre l'intrusion et la reprise de contrôle. On part du principe qu'on sera attaqué : l'enjeu devient la vitesse de détection et de réaction.

Leviers

Centralisation des logs, monitoring et alerting, plan de réponse à incident écrit (qui fait quoi, qui on appelle), chaîne d'escalade, exercices de crise pour tester le plan, et option d'un SOC / EDR managé (MDR) pour surveiller proactivement

09 - Gouvernance & conformité

→ Le cadre formel qui transforme des mesures éparses en système piloté, et qui tient vos obligations.

Rôle

Passer de « on se protège » à « on pilote et on prouve » — ce qui rassure clients, investisseurs et assureurs et vous permet de cartographier le risque

Leviers

Politique de sécurité documentée, cartographie des risques et des surfaces, gestion des risques, conformité RGPD ou NIS2, certifications selon votre marché (ISO 27001, SOC 2, HDS), gestion des fournisseurs et des tiers, plan de continuité et de reprise (PCA / PRA), et cyber-assurance.

10 - Données & sauvegardes

→ La donnée est l'actif final que tout le reste protège — encore faut-il savoir où elle vit et pouvoir la récupérer en cas d'incident.

Rôle

La dernière ligne. Quand tout le reste a cédé — ransomware, suppression, sinistre — c'est votre capacité à restaurer qui décide si l'entreprise survit ou non.

Leviers

Cartographier où vivent les données (serveurs, Drive, CRM, SaaS), assurer les sauvegardes, tester les restaurations — une sauvegarde jamais restaurée n'existe pas. Et M365 et Workspace ne sont pas des sauvegardes.