Wico Réseau

ENTRE MYTHE & RÉALITÉ

Comment mieux anticiper, prévenir et surmonter une **cyberattaque** en 2026 ?

Le guide pratique qu'il vous faut pour anticiper vos risques cyber !



AU PROGRAMME

Introduction : Mythes et réalités de la cybersécurité en 2026 3

I – L'État de la menace : chiffres clés et secteurs cibles 4
- Les indicateurs alarmants du marché
- Focus sur l'évolution des secteurs cibles

II – En Amont : Les actions préventives (éviter l'intrusion) 5
- Généraliser l'authentification multifacteur
- Compartimenter l'infrastructure réseau
- Remplacer l'antivirus traditionnel par un EDR
- Sensibiliser le facteur humain

III – En Aval : protocole d'urgence de la première heure 6
- Isoler physiquement sans éteindre
- Protéger les supports de sauvegarde
- Déclencher l'alerte d'ingenierie

IV – Le cadre légal : vos obligations sous 72 Heures 7
- Dépôt de plainte
- Notification à la CNIL
- Déclaration de sinistre

V – Solutions illico réseau 8
- Audit et diagnostique
- Sauvegarde
- Supervision proactive

Conclusion & Recommandations 9

MYTHES ET RÉALITÉS DE LA CYBERSÉCURITÉ

Dans un paysage économique hyper-connecté, **la cybersécurité n'est plus un simple sujet** technique relégué aux équipes informatiques : **c'est un enjeu vital de gouvernance et une obligation légale de conformité** (notamment sous l'impulsion de la directive NIS 2 et de la loi LOPMI). Pourtant, de nombreux dirigeants de PME et d'ETI partagent encore des croyances obsolètes.

Mythe n°1

« Mon entreprise est trop petite pour intéresser les hackers. »

Réalité

En 2026, les attaques sont automatisées via des bots de balayage. Les PME sont des cibles privilégiées car elles possèdent souvent des défenses moins matures et servent de passerelles pour compromettre leurs grands donneurs d'ordres. **Avec la directive NIS 2, la sécurité des sous-traitants devient d'ailleurs une exigence contractuelle et légale incontournable.**

Mythe n°2

« J'ai un bon antivirus et mes données sont dans le Cloud, je ne risque rien. »

Réalité

Les ransomwares modernes désactivent les antivirus standards en quelques secondes et chiffrent directement les environnements Cloud non segmentés. De plus, en cas de sinistre, **la loi LOPMI conditionne tout dédommagement d'assurance à un dépôt de plainte sous 72 h** et interdit la couverture financière des rançons sans procédure formelle.

L'objectif de ce guide est de vous apporter une visibilité claire en distinguant les faits des idées reçues, tout en vous fournissant une feuille de route actionnable **pour sanctuariser votre activité et assurer votre mise en conformité réglementaire partout dans le Grand Ouest.**

I – L'ÉTAT DE LA MENACE : CHIFFRES CLÉS ET SECTEURS CIBLES

La cybersécurité n'est plus seulement un sujet de protection des actifs informatiques : c'est une **exigence réglementaire et de gouvernance pilotée par l'ANSSI notamment via la directive européenne NIS 2 et la loi LOPMI.** Les réglementations imposent une responsabilité directe et accrue aux dirigeants de PME, d'ETI et de collectivités.. Les directives européennes et le droit français imposent une responsabilité accrue aux dirigeants de PME, d'ETI et de collectivités.

Les indicateurs alarmants du marché :

40%

des entreprises françaises

déclarent avoir subi au moins une tentative d'intrusion ou une attaque par phishing au cours des 12 derniers mois.

Selon le CESIN - Baromètre annuel

2/3

attaques par rançongiciel

visent spécifiquement les structures de taille moyenne (PME et collectivités) sur les trois dernières années.

Selon l'ANSSI - Rapport annuel

60%

des PME

touchées par un vol massif de données ou un arrêt d'activité prolongé de plus de 5 jours déposent le bilan dans les 6 mois qui suivent le sinistre.

Selon l'ANSSI

Focus sur l'évolution des secteurs cibles :

Santé et structures médico-sociales

Les hôpitaux et cliniques restent en première ligne. Leurs données de santé se revendent au prix fort sur le darknet, et leur faible tolérance aux interruptions pousse les attaquants au chantage — **secteur prioritaire NIS 2.**

Logistique, Transport et Industrie

Des secteurs dépendants de flux d'informations en temps réel. Un blocage des serveurs de supply chain paralyse immédiatement les livraisons et les chaînes de production. Sous NIS 2, **la sécurisation de la chaîne de sous-traitance (supply chain) devient un impératif contractuel.**

Collectivités et Services Publics

Souvent ciblés pour bloquer les services aux usagers ou exfiltrer des bases de données citoyennes sensibles **(obligations renforcées de notification sous 24h à l'ANSSI).**

II – EN AMONT : LES ACTIONS PRÉVENTIVES (ÉVITER L'INTRUSION)

Une cybersécurité efficace n'est pas réactive : elle se construit au jour le jour pour **neutraliser 90% des menaces de masse** avant qu'elles n'atteignent le cœur de votre réseau, en application directe du guide d'hygiène informatique de l'ANSSI et des exigences de la directive NIS 2.

1. Généraliser l'authentification multifacteur (MFA / 2FA)

Référence légale : Règle 12 du guide d'hygiène ANSSI / RGPD (Art. 32)

L'usurpation d'identifiants par phishing reste la porte d'entrée majeure. Le MFA exigé par l'ANSSI et rendue obligatoire par la directive NIS 2 pour tous les accès distants et administratifs, **la double authentification bloque 99 % des tentatives d'intrusion** fondées sur des identifiants compromis.

2. Compartimenter l'infrastructure réseau (VLAN)

Référence légale : Règle 12 du guide d'hygiène ANSSI / RGPD (Art. 32)

Ne laissez pas l'intégralité de vos systèmes sur la même voie. Recommandée par l'ANSSI et alignée sur l'article 32 du RGPD (sécurité du traitement), **la segmentation en VLANs étanches (Administratif, IoT, Invités, Production) empêche la propagation latérale d'un rançongiciel** vers vos serveurs critiques ou vos bases de données clients

3. Remplacer l'antivirus traditionnel par un EDR

Référence légale : Surveillance active et détection continue (NIS 2 / DORA).

Les logiciels malveillants de 2026 contournent facilement les signatures des antivirus classiques. Pour satisfaire aux exigences européennes de surveillance et de détection précoce des incidents, **l'EDR analyse les comportements anormaux en temps réel et isole automatiquement les postes infectés** avant l'exfiltration de données.

4. Sensibiliser le facteur humain

Référence légale : Obligation de formation des personnels et dirigeants (Directive NIS 2).

Vos équipes sont vos meilleurs boucliers. Inscrite comme une obligation légale de gouvernance sous NIS 2, **la formation régulière des équipes et les simulations de phishing permettent de réduire le risque d'erreur humaine,** à l'origine de plus de 80 % des intrusions.

III – EN AVAL : PROTOCOLE D'URGENCE DE LA PREMIÈRE HEURE

Si une faille de sécurité est exploitée malgré vos protections, les actions menées dans les 60 premières minutes sont critiques pour limiter la propagation.

Isoler physiquement sans éteindre

Débranchez immédiatement les câbles réseau (Ethernet) de toutes les machines et coupez les routeurs Wi-Fi. **NE REDÉMARREZ PAS ET N'ÉTEIGNEZ PAS LES MACHINES.** Forcer l'extinction écrase les données volatiles de la mémoire vive (RAM), **privant les experts des clés de déchiffrement et rendant les preuves numériques irrecevables** auprès des enquêteurs et des assurances.

Protéger les supports de sauvegarde

Déconnectez immédiatement les disques durs externes et serveurs NAS branchés au réseau pour éviter qu'ils ne soient ciblés.

Déclencher l'alerte d'ingénierie

Contactez immédiatement votre prestataire informatique de confiance. Les analystes de sécurité prennent le contrôle de vos flux périmétriques pour cartographier l'attaque, tout en initialisant le **rapport d'incident technique exigé sous 24h par l'ANSSI** (directive NIS 2).

Exemple de terrain

En mai dernier, une entreprise de logistique basée dans le Grand Ouest a subi l'activation d'un ransomware à 14h. **Grâce à l'application stricte de ce protocole (débranchement instantané des commutateurs réseau)**, l'attaque a été circonscrite à 3 ordinateurs. Les serveurs centraux et l'ERP de l'entreprise ont été sauvés, **évitant un chantage à 120 000 € et garantissant la totale conformité de l'entreprise vis-à-vis de l'article L.12-10-1 de la loi LOPMI** (interdisant tout remboursement d'assurance sans déclaration formelle).

IV – LE CADRE LÉGAL : VOS OBLIGATIONS SOUS 72 HEURES

Faire l'objet d'une cyberattaque implique des responsabilités juridiques strictes. Depuis l'entrée en vigueur de la loi LOPMI, le non-respect des démarches déclaratives prive l'entreprise de tout remboursement d'assurance et l'expose à de lourdes sanctions réglementaires.

Démarche obligatoire

Dépôt de plainte officielle

Loi LOPMI (Art. L. 12-10-1 du Code des assurances)

Sous 72 Heures

À effectuer auprès du commissariat ou de la gendarmerie. Cette démarche sous 72 h **est la condition légale obligatoire** sans laquelle les cyber-assurances pourraient interdire la couverture financière.

Délai réglementaire

Notification à la CNIL

RGPD (Art. 33)

Sous 72 Heures

Obligatoire dès lors qu'il existe un risque pour les droits des personnes (fuite ou chiffrement de coordonnées clients, RIB, fiches de paie). Le non-respect de ce délai expose l'entreprise à des sanctions de la CNIL pouvant atteindre jusqu'à 4 % du chiffre d'affaires mondial.

Objectif & Description

Déclaration de sinistre Assureur

Code des Assurances (Art. L. 113-2)

24h à 48h

Permet de débloquer immédiatement l'assistance technique et financière de gestion de crise (intervention d'experts en négociation et reconstruction, prise en charge des frais juridiques et pertes d'exploitation).

Notification ANSSI (Directive NIS 2)

Pour les entités et sous-traitants régulés : obligation d'une alerte précoce sous 24 h à l'ANSSI en cas d'incident significatif, suivie d'une notification formelle sous 72 h.

V – SOLUTIONS ILLICO RÉSEAU : AUDIT ET SUPERVISION CONTINUE

Pour vous accompagner face à ces défis, **Illico Réseau déploie des solutions souveraines de pointe, adaptées à la réalité opérationnelle des entreprises** de l'ensemble du Grand Ouest et alignées sur les exigences de l'ANSSI et de la directive NIS 2.

Audit et diagnostic des infrastructures

Nous analysons vos configurations réseau, scannons vos vulnérabilités et évaluons la robustesse de vos processus d'accès selon les référentiels de l'ANSSI pour **identifier vos failles avant les attaquants et anticiper votre mise en conformité réglementaire.**

Sauvegardes immuables et externalisées

Nous mettons en place des sauvegardes automatisées non réécritibles (immuables) stockées hors de vos infrastructures physiques, suivant la règle 3-2-1 exigée par les cyber-assurances et les normes de résilience (DORA / NIS 2). **En cas d'attaque totale, nous pouvons reconstruire votre environnement sans jamais négocier avec les pirates.**

Supervision proactive par console SOC

Grâce à notre centre opérationnel de sécurité (SOC), vos réseaux professionnels font l'objet d'une surveillance continue. **Nos ingénieurs analysent les alertes de criticité en temps réel** pour détecter les signaux faibles et intervenir de manière chirurgicale avant la propagation, r**épondant ainsi à l'obligation de détection et de signalement précoce d'incidents.**

RECOMMANDATIONS FINALES

La cyber-résilience moderne n'est pas une simple option technique : **c'est l'assurance vie et la garantie de conformité légale (NIS 2 / RGPD / LOPMI) de votre entreprise.** Elle exige la combinaison d'une excellente hygiène préventive en amont et d'une réactivité méthodique en aval.

N'attendez pas d'être la cible d'une attaque pour évaluer vos barrières de protection. Prenez les devants, protégez vos collaborateurs et sécurisez vos infrastructures dès aujourd'hui.

Un doute sur la conformité de vos installations ?

Planifiez votre audit de sécurité avec nos équipes.

Standard
02 22 54 24 30

contact@illico-reseau.com

Illico Réseau

Prestataire Réseaux, Connectivité & Cybersécurité dans le Grand Ouest

Angers Nantes

www.illico-reseau.com

