INFORSUD
TECHNOLOGIES
Solutions et impulsions pour l'avenir

GUIDE PRATIQUE

La cybersécurité, maillon essentiel de la transformation numérique

Sommaire

« La cybersécurité est un levier d'avenir positif et non un mal nécessaire ! Elle apporte de la valeur par la confiance qu'elle procure en sécurisant les outils et usages autour du numérique. »

Etienne de Séréville, IBM pour la commission cybersécurité de Numeum

CYBERSÉCURITÉ

Introduction

Le numérique continue de transformer l'économie en profondeur. Sans pour autant abolir un élément immuable à tout type d'économies : le besoin de confiance. Une confiance qui s'appuie sur des outils, processus et bonnes pratiques pour assurer la sécurité des systèmes d'informations.

En 2021, plus d'une entreprise sur deux déclare avoir subi entre une à trois cyberattaques abouties, avec des répercussions tangibles, selon l'enquête OpinionWay 2021 pour le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN).

Un chiffre à relativiser toutefois : si l'exposition à des attaques est importante, les apports du numérique (amélioration des processus, automatisation de certaines tâches chronophages, excellence opérationnelle…) sont largement supérieurs aux risques cyber.

L'objectif de la cybersécurité est avant tout de gagner en efficacité et sérénité, dans une démarche pragmatique et équilibrée, ni anxiogène ni angélique. C'est tout l'objet de ce guide, dans lequel vous découvrirez ou redécouvrirez :

- Les principaux risques, menaces et les objectifs des cyberattaquants ;
- Les solutions dédiées et leur intégration à l'écosystème de toute l'organisation ;
- Les bonnes pratiques et méthodes de gouvernance adaptées ;
- L'importance de la sensibilisation et le rôle déterminant des utilisateurs dans la sécurité numérique.

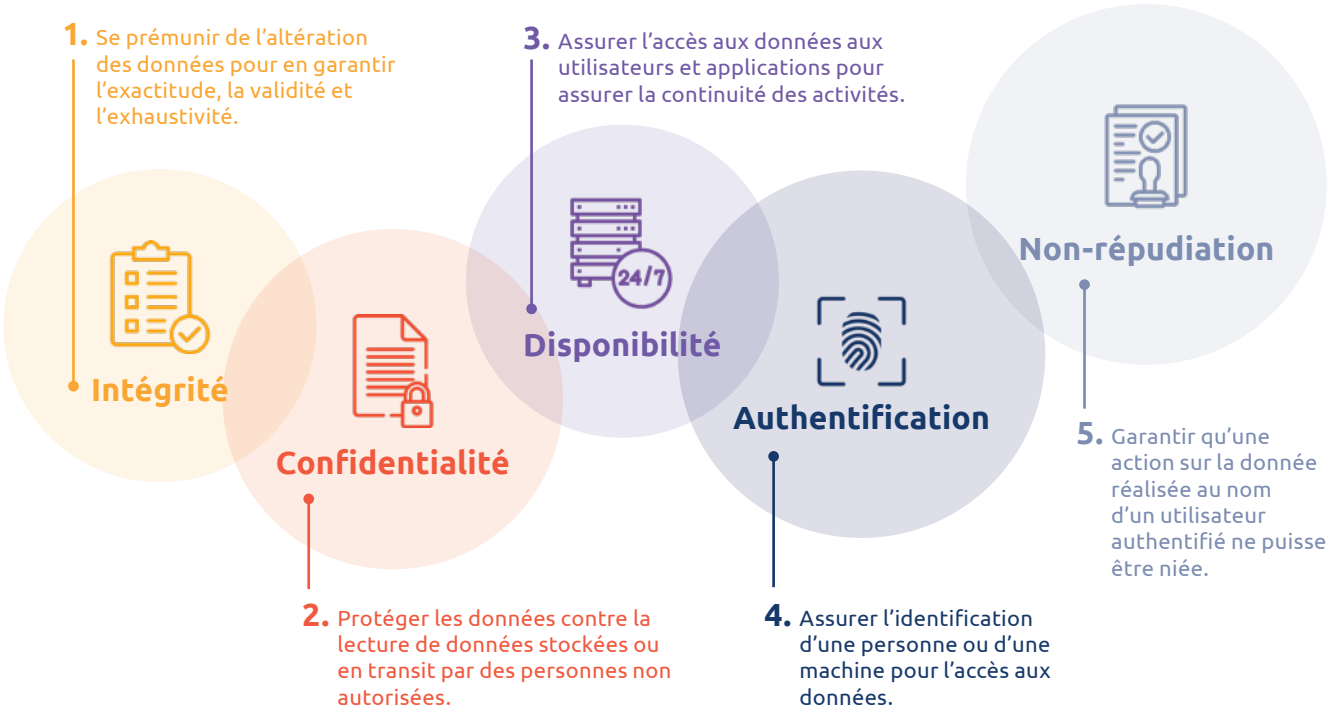
Les principaux enjeux de la cybersécurité

Bien que la cybersécurité diffère sensiblement selon les tailles d'organisation, leur secteur et leur niveau de maturité digitale, la sécurisation de l'écosystème numérique vise avant tout à protéger les données car ce sont elles qui portent la valeur ajoutée de l'organisation.

Les données à protéger :

- Peuvent être de nature différente (informations clients, commandes, facturation, méthodes et secrets de fabrication, RH…) ;
- Ont différents niveaux de criticité et de temporalité (leur valeur évolue dans le temps) ;
- Sont potentiellement encadrées au niveau réglementaire (exemple : les données personnelles RGPD) ;
- Sont structurées (base de données), semi-structurées (métadonnées et balises sémantiques de documents, par exemple) ou non structurées (e-mails, Word, Excel, PowerPoint, réseaux sociaux, etc.)

Les 5 objectifs de la cybersécurité



Les risques en cas d'attaque

- **Arrêt d'activité :** arrêts de production, retards...
- **Risque industriel :** IoT, chaîne industrielle intégrée...
- **Risque économique :** pertes de CA, sanctions financières...
- **Image de marque :** données clients, partenaires...
- **Risque juridique :** RGPD, cyber assurances...
- **Espionnage économique :** secrets de fabrication, vol de brevets..

Quelques chiffres clés

95% des atteintes à la cybersécurité sont d'origine humaine.

60% des entreprises attaquées ont été impactées sur leur activité.

14% par la compromission de données.

21% en raison d'une perturbation de la production.

×4 est le facteur de multiplication des ransomwares.

70% des structures ont payé des rançons. Seule la moitié a récupéré des données.

35000€ est le coût moyen d'une cyberattaque en France en 2020 contre 9 000 € en 2019.

Sources : ETC Technologies ; ANSSI 2020 ; CESIN 2021 ; Revue nationale de la gendarmerie 2021

FOCUS

L'arnaque au président toujours très fréquente

Ce type de fraude vise à convaincre le collaborateur de tout type d'organisation, d'effectuer en urgence un virement à un tiers pour obéir à un prétendu ordre du dirigeant, sous prétexte d'une dette à régler, de provision de contrat ou autre.

POINT DE VIGILANCE

S'assurer contre le risque cyber : oui, sans négliger la prévention !

Face à un risque nouveau, les offres assurantielles en matière cyber n'ont pas tardé à apparaître sur le marché contre les risques identifiés : fuite de données, pertes d'exploitation, rançon (qu'il est fortement déconseillé de payer), etc.

Pour autant, la première des protections demeure la prévention, afin de se prémunir des attaques et des risques associés.

Les aspects techniques

Les attaquants sont inventifs. Mais ils vont aussi à la facilité pour obtenir un maximum de gains dans un laps de temps le plus court possible. Même s'il est impossible de se prémunir à 100 %, un travail de fond en matière de protection du système d'information (réseaux, postes de travail, serveurs…) permet d'endiguer les flux cybercriminels majeurs.

1 Mettre à jour son parc applicatif : le socle de la cybersécurité

Les mises à jour logicielles, et notamment celles corrigeant des failles de sécurité découvertes sur les systèmes d'exploitation, les applicatifs (postes et serveurs) et bien sûr les antivirus, sont un des piliers de la sécurité dans les organisations.

Le délai de mise à jour doit être le plus court possible, même pour les collaborateurs en mobilité. Avec des solutions avancées de gestion de parcs IT, les mises à jour peuvent désormais s'opérer à distance.

2 Déployer des outils de protection adaptés*

- L'antivirus, encore utile mais aujourd'hui insuffisant ;
- le VPN, pour sécuriser les flux de données entre le réseau et les postes distants ;
- le firewall, pour sécuriser au maximum le périmètre du SI ;
- la gestion des identités et des accès, pour garantir l'identité des utilisateurs et les droits dont ils disposent ;
- les solutions EDR/XDR, pour détecter les comportements anormaux des éléments du SI (postes de travail, serveurs, etc.), en remplacement des antivirus moins efficaces.

3 Sécuriser le télétravail et le nomadisme

Sans maîtrise du réseau, les dangers sont plus nombreux. L'utilisation des VPN est une réponse mais c'est loin d'être la seule. Des efforts sont également à fournir sur la sécurité embarquée (double authentification, par exemple).

De la même façon, l'utilisation de Wifi publics est à proscrire. Même dans les hôtels (avec authentification), il est impossible de connaître le niveau de sécurité du réseau. Le partage réseau 4G/5G depuis son smartphone reste encore la meilleure solution.

*Liste non exhaustive

FOCUS

L'analyse comportementale et l'apprentissage automatique, complément au traditionnel antivirus

En complément de l'antivirus, capable d'identifier et de bloquer les attaques connues, les solutions EDR/XDR, basées sur l'analyse des comportements et l'apprentissage automatique (intelligence embarquée), sont en mesure de contrer tout type d'attaque (« Zero-day », « Fileless », « Sandboxing » dans le cloud …) et demeurent plus efficaces, notamment au sein d'un périmètre ouvert et étendu (cloud, nomadisme, etc.).

Solutions EDR

Surveillance des terminaux (endpoints en anglais) : ordinateurs, tablettes, téléphones portables… mais pas du réseau du système d'Information.

Solutions XDR

Analyse des données de l'ensemble de l'éco-système, provenant de sources multiples : terminaux, serveurs, réseaux **et surtout de tous les flux cloud.**

4 Organiser sa résilience : la sauvegarde de données

En cas d'attaque réussie, la sauvegarde de données garantit à l'organisation de continuer ou reprendre ses activités en subissant le moins de pertes possibles, dans le cadre d'un plan de sauvegarde conformes aux enjeux, contraintes et criticités de l'organisation.

Très schématiquement, un plan de sauvegarde des données doit respecter la règle dite du « 3-2-1-0 » :

- disposer de **trois** exemplaires de ses données : un original et deux sauvegardes ;
- conserver ces sauvegardes sur **deux** supports différents, pour éviter les pannes communes ;
- stocker l'une des sauvegardes dans **un** autre emplacement physique ;
- garantir **zéro** erreur, en testant régulièrement les restaurations.

5 Tester sa résistance

Les outils de cybersécurité sont indispensables. Mais il faut tester régulièrement la résistance aux attaques pour ne pas compromettre les investissements réalisés pour protéger le SI. Nous recommandons de tester au moins une fois tous les 2 ans pour une PME.

L'audit de sécurité

L'audit de sécurité est un passage en revue de l'ensemble de l'infrastructure (réseaux, applications, failles de sécurité, erreurs de configuration…), des comportements et des usages.

Son objectif : identifier les éventuels points de faiblesse sur des aspects techniques ou procéduraux, afin de les corriger et ainsi limiter la surface d'attaque potentielle de l'entreprise.

Les pentests

Le test de pénétration a pour fonction de cibler des composants de l'infrastructure afin de vérifier leur robustesse. Il se déroule en quatre étapes :

- analyse de l'infrastructure, de l'application et/ou de la technologie,
- identification des failles,
- exploitation des vulnérabilités,
- analyse de l'impact dans l'organisation.

À noter que les pentests sont à renouveler régulièrement, afin de s'assurer de la robustesse des solutions de remédiation déployées, et d'identifier l'émergence de nouvelles failles.

POUR ALLER PLUS LOIN

L'approche Zéro Trust Network : la sécurité des SI ouverts et étendus

L'approche ZTN a déplacé le périmètre de sécurité des frontières du SI vers le trinôme utilisateurs / machines / applications, qui doivent être authentifiés pour agir sur le SI. Par exemple, un utilisateur légitime qui tente de se connecter à partir d'une machine non authentifiée n'accédera pas au réseau.

Les principaux piliers de la démarche ZTN : les outils de **gestion des accès et des identités**, le principe du **moindre privilège** et le **chiffrement des flux**.

Pour en savoir plus sur la mise en œuvre d'une politique de sauvegarde efficace, téléchargez notre guide pratique « La sauvegarde de données : une assurance incontournable », en scannant le QR Code ou en cliquant sur ce lien.

Les aspects humains

Malgré toutes les protections techniques mises en œuvre en matière de cybersécurité, l'humain reste le maillon le plus faible de la chaîne. Dans la grande majorité des cas, les compromissions avérées sont le fruit d'une négligence ou d'une erreur humaine : clic sur des liens malveillants, utilisation d'un réseau Wifi non sécurisé, etc.

Pour 73 %
des entreprises le phishing reste le vecteur d'attaque le plus fréquent
Source : CESIN

Les risques & enjeux

– L'ingénierie sociale en constante augmentation

L'ingénierie sociale est un ensemble de techniques de manipulation utilisées par les cybercriminels pour inciter les utilisateurs à partager des informations confidentielles :

- Messagerie : phishing (envoi d'e-mails frauduleux)
- Navigation web : sites contrefaits pour récupérer des informations personnelles
- Acquisition frauduleuse d'informations sur les réseaux sociaux

– Le nomadisme

En mobilité lors de déplacements et en télétravail, les risques sont décuplés :

- Multiplication des terminaux : téléphones portables, périphériques amovibles et mobiles
- Réseaux potentiellement non sécurisés (Wifi public)
- Utilisation accrue d'équipements personnels

– Les mots de passe

La fonction des mots de passe est d'authentifier un utilisateur souhaitant accéder à tel ou tel applicatif. Parmi les bonnes pratiques à respecter

- Une obligation de robustesse (nombre de signes, signes alphanumériques, caractères spéciaux, etc.)
- Un changement régulier
- Un mot de passe différent par application, y compris dans le domaine personnel

– L'environnement de travail

Les risques cyber ne sont pas l'apanage des postes fixes ou portables et de l'usage qui en est fait. D'autres vecteurs d'attaques sont possibles :

- Les ports USB et chargeurs des postes
- Les imprimantes
- Les disques durs, etc.

– Les mises à jour des postes de travail

Au même titre que les serveurs de l'entreprise, les postes de travail doivent bénéficier des mises à jour dans des délais courts : malgré toute la bonne volonté des utilisateurs, les failles de postes qui n'ont pas été mis à jour (système d'exploitation, logiciels / applis, navigateurs, plug-ins, etc.) sont autant de portes ouvertes sur le SI.

FOCUS

Le phishing, principale menace de la « famille » ingénierie sociale

Phishing : à partir d'un e-mail hameçon, leurrer des utilisateurs à l'aide d'un faux site (de plus en plus réaliste) pour l'inciter à divulguer des identifiants de connexion, des informations financières, etc.

Spear phishing : variante du phishing visant précisément un individu ou un petit groupe d'individus, à l'aide d'informations spécifiques les concernant.

ASTUCE

Le gestionnaire de mots de passe

Imposer des changements de mot de passe réguliers est une pratique recommandée mais contraignante. Bien qu'avec de la pédagogie, il est possible de renforcer le taux d'acceptation, l'utilisation d'un gestionnaire de mots de passe chiffrés demeure la **meilleure arme pour garantir l'usage des bonnes pratiques en matière de mots de passe**, avec une authentification unique pour accéder à toutes les applications et ressources.

Gestionnaires conseillés : Kpass (gratuit et recommandé par l'ANSSI*) ou Keeper (payant et granulaire) qui permet de gérer les mots de passe entre plusieurs personnes d'un même service par exemple.

Les bonnes pratiques

1 Sensibiliser et former les utilisateurs

Expliciter les dangers, les méthodes des attaquants et répéter les bonnes pratiques pour s'en prémunir au quotidien est un élément clé de la cybersécurité.

Cela passe par des formations, de l'information régulière pour sensibiliser TOUS les collaborateurs et fédérer tous les acteurs de l'organisation autour des enjeux de sécurisation :

- Y compris les plus hautes fonctions, qui sont les plus exposées et qui disposent des accès les plus importants.
- En insistant sur les risques accrus liés au développement du télétravail, où les comportements peuvent se relâcher.

2 Équiper les collaborateurs pour séparer les usages professionnels et personnels

Avec le développement du télétravail et du nomadisme, le mélange des usages professionnels et personnels des terminaux s'accroit : utilisation de postes personnels pour accéder au SI (configuration de sécurité non maîtrisée), postes professionnels utilisés à des fins personnelles, smartphones (souvent mal sécurisés).

Pour garantir la sécurité maximale, donner accès aux télétravailleurs ou personnels nomades, à des postes ou environnements de travail sécurisés est la réponse la plus pertinente. Avec là aussi, une certaine sensibilisation des utilisateurs afin qu'ils utilisent leurs postes à des fins professionnelles uniquement.

3 Adopter la politique du moindre privilège

Les comptes à privilèges comme les administrateurs du système d'information, sont les plus exposés et les plus dangereux : en cas de compromission, ils permettent d'accéder à tout ou à une très grande partie du système d'information.

- L'utilisation de mots de passe forts est particulièrement recommandée pour ces comptes.
- Il est recommandé de limiter ce type de comptes, selon le principe du moindre privilège (POLP).

LE BON RÉFLEXE

Briser les tabous : vérifier et alerter au moindre doute

L'erreur est humaine et peut arriver à tout le monde à tout moment. La cacher empire les choses. La consigne aux utilisateurs doit être claire : en cas de doute, informer immédiatement le service informatique. Les conséquences seront forcément moins graves qu'une erreur avérée non déclarée.

Onéreux, le déploiement et la gestion d'un ordinateur portable sécurisé par collaborateur le sont toutefois moins que les dégâts encourus (pertes d'exploitation, image, etc.).

*ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

Le risque zéro n'existe pas !

Quels que soient les outils et les bonnes pratiques mises en œuvre pour sécuriser le système d'information, le risque zéro n'existe pas compte tenu de l'évolution des menaces et de la créativité des attaquants. La question désormais n'est plus de savoir si on sera une cible, mais quand on le sera, et comment on réagira.

Il faut donc préparer des procédures spécifiques à suivre en cas de cyberattaque. La réponse n'est pas uniquement technique pour limiter la propagation en cas d'attaque : elle doit intégrer les dimensions juridique, commerciale, opérationnelle et humaine.

Pour évaluer les risques et augmenter son niveau de sécurité, une organisation doit par ailleurs prendre en compte l'ensemble de son écosystème : sous-traitants, partenaires, clients, fournisseurs, prestataires…

En cas d'attaque : adoptez les bons réflexes !

- **Alertez immédiatement votre support informatique** afin qu'il prenne en compte l'incident : service informatique interne, prestataire, personne en charge de la sécurité.
- **Isolez les systèmes attaqués** afin d'éviter que l'attaque ne puisse se propager à d'autres équipements en coupant toutes les connexions à Internet et au réseau local. **Déconnectez vos supports de sauvegarde** et laissez éteints les équipements non démarrés.
- **Constituez une équipe de gestion de crise** afin de piloter les actions des différentes composantes concernées : technique, RH, financière, communication, juridique, etc.
- **Tenez un registre des événements et actions réalisées** pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.
- **Préservez les preuves de l'attaque :** messages reçus, machines touchées, journaux de connexions, etc.
- **Déposez plainte avant toute action de remédiation** en fournissant toutes les preuves en votre possession.
- **Déclarez le sinistre auprès de votre assureur** qui peut vous dédommager voire vous apporter une assistance en fonction de votre niveau de couverture assurantielle.
- **Alertez votre banque** au cas où des informations permettant de réaliser des transferts de fonds auraient pu être dérobées.
- **Gérez votre communication afin d'informer avec le juste niveau de transparence** vos administrés, clients, collaborateurs, partenaires, fournisseurs, médias, etc.
- **Ne pas payer de rançon :** son paiement ne garantit aucun résultat et motivera les assaillants à vous attaquer une autre fois.
- **Faites-vous accompagner par des prestataires spécialisés en cybersécurité**.

Source : www.cybermalveillance.gouv.fr.

INFORSUD
TECHNOLOGIES

Solutions et impulsions pour l'avenir

INFORSUD Technologies

Solutions et impulsions pour l'avenir

Prestataire de services informatiques basé en Occitanie, nous accompagnons les entreprises et collectivités dans leur transformation numérique, avec une offre qui couvre tous leurs besoins : conseil et aide au choix, gestion et évolution d'infrastructures IT en local ou hébergées dans le Cloud, gestion des postes de travail, cybersécurité, solutions de gestion - paie - RH, développements spécifiques.

Notre savoir-faire depuis plus de 35 ans et notre accompagnement de proximité nous permettent d'apporter à nos 380 clients l'impulsion technologique nécessaire, et de les aider à optimiser leurs processus métiers durablement, grâce au numérique.

Du lundi au vendredi 8h30-12h30 et 13h30-17h30 **Numéro unique** **0 811 349 609**

Agence Haute-Garonne
2, rue Maryse Hilsz
31500 Toulouse

Agence Tarn
Impasse des Crins
81990 Le Sequestre

Siège Social
Causse Comtal
12340 Bozouls

contact@inforsud-technologies.com
inforsud-technologies.com