Cybersécurité: ce qui change pour chacun d’entre nous

12 décembre 2025

Cette conférence, organisée dans le cadre des petits-déjeuners du Lab’ de #VivaIssy, aborde le thème de la cybersécurité, un sujet qui a transcendé le cercle des experts pour concerner chaque citoyen, entreprise et institution. L'objectif est de comprendre les menaces actuelles, les changements en cours et les moyens de protection disponibles.

État des lieux de la cybersécurité

Pierre Lagarde, CTO Microsoft France, a détaillé les principales tendances observées dans le rapport annuel mondial de Microsoft, *Digital Defense,* sur les risques et menaces cyber. Cette présentation se déroule en trois étapes : un état des lieux, le partage de chiffres clés et un focus sur l'intelligence artificielle (IA).

Positionnement de la France et cibles principales

- La France ne figure pas dans le top 10 des pays les plus ciblés au niveau mondial, se classant au 12ème rang selon les observations de Microsoft. Cependant, elle occupe la 4ème place au niveau européen.
- Industries les plus ciblées en France sont :
    - Les hôpitaux
    - Les écoles publiques
    - Les collectivités locales
- Cause principale :Cette vulnérabilité s'explique principalement par l'obsolescence du matériel utilisé dans ces institutions. Le matériel est

souvent ancien, non mis à jour, et donc plus facile à cibler pour les attaquants.

Les attaques étatiques

Les attaques menées par des États constituent un élément important du paysage de la cybersécurité. Quatre pays sont identifiés comme étant les plus actifs :

- La Chine et l'Iran :Leurs activités se concentrent principalement sur l'espionnage, qui ne représente qu'un faible pourcentage de l'ensemble des cyberattaques.
- La Russie: Ses attaques sont quasi exclusivement focalisées sur l'Ukraine.
- La Corée du Nord utilise une méthode d'attaque particulière qui consiste à envoyer des travailleurs dans des entreprises mondiales à l'étranger. Ces "émissaires" collectent des informations et les rapportent à leur pays.

La priorité numéro un : la cybersécurité

La conclusion principale de cet état des lieux est que la cybersécurité doit être une priorité absolue pour toutes les organisations, qu'elles soient professionnelles ou citoyennes. L'axe d'attaque principal reste l'identité et les mots de passe, ce qui souligne l'importance des bonnes pratiques individuelles et collectives.

Chiffres clés et nature des attaques

Motivations et méthodes des attaquants

- L'extorsion et le ransomware :Ces types d'attaques représentent une attaque sur deux. Le but principal des attaquants est de voler des données pour les revendre. La cyberattaque est un véritable "business" dont l'objectif est de générer de l'argent.
- Le vol de données :80 % des attaques visent à voler des données.
- La porte d'entrée :Contrairement à l'image véhiculée par le cinéma, les attaquants n'exploitent que rarement des failles complexes ou des portes dérobées. 97 % des attaques se font par la "porte d'entrée", c'est-à-dire en utilisant un identifiant et un mot de passe. Ils exploitent la réutilisation de mots de passe identiques ou l'utilisation de mots de passe simples.

Pour contrer ces menaces, Microsoft analyse un volume massif de données :

- 100 000 milliards de signaux sont analysés quotidiennement. Cette capacité d'analyse provient de la diversité de l'écosystème Microsoft, qui inclut le jeu vidéo (Xbox), les services grand public (Hotmail, Outlook.com) et les services d'entreprise (Cloud, Microsoft 365).
- **Filtrage des menaces :**
    - 5 milliards d'e-mails malveillants sont retirés chaque jour.
    - 4,5 millions de fichiers contenant des virus sont supprimés quotidiennement.

Sur plus de 120 000 employés chez Microsoft, 34 000 personnes travaillent dans l'entité cybersécurité. Ces équipes ne sont pas uniquement composées d'ingénieurs. On y trouve également :

- Des spécialistes en politique (pour l'aspect géopolitique).
- Des linguistes (pour analyser les langues spécifiques utilisées).
- Des sociologues.

Les failles de la sécurité par mot de passe et les solutions actuelles

La faiblesse des mots de passe et l'importance de la double authentification

- L'humain comme maillon faible : Une attaque réussie contre 130 communes françaises a été rendue possible parce qu'une secrétaire de mairie utilisait le même mot de passe pour ses comptes professionnel et personnel, ce dernier ayant été compromis. Un autre exemple mentionne la compromission d'un mot de passe par défaut qui n'avait pas été changé.
- La double authentification comme parade : Il est estimé que 98 % des attaques par mot de passe pourraient être évitées si la double authentification était systématiquement activée. Ce système, de plus en plus courant, utilise diverses méthodes :
    - SMS
    - E-mail
    - Application d'authentification (type Authenticator)

L'émergence des systèmes "sans mot de passe"

En réponse à la faiblesse que peut représenter la double authentification elle-même, une campagne a été menée pour promouvoir les environnements "sans mot de passe". Le fonctionnement est le suivant :

1. L'utilisateur clique sur "je m'authentifie" et entre son adresse e-mail.
2. Il reçoit une notification sur son téléphone avec un numéro à valider.
3. L'authentification se fait en une seule étape via un autre appareil (PC ou téléphone), éliminant ainsi le besoin de mémoriser ou de saisir un mot de passe.

Le changement de paradigme : la cybersécurité comme levier stratégique

Thomas Hervouet-Kasmi, Président de l'association de veille stratégique INNOCHERCHE, expose comment la cybersécurité est passée d'un centre de coûts à un facteur stratégique essentiel.

Présentation de l'association INNOCHERCHE

- Mission :Aider la société à prendre du recul sur les sujets technologiques.
- Domaines d'expertise :Observatoires de veille sur la cybersécurité, l'IA, la Smart City.
- Activités :Conférences, jeu de sensibilisation à la cybersécurité, cycles de travail sur l'identité numérique et l'IA sécurisée.

De centre de coûts à pilier stratégique

- La cybersécurité était perçue comme un simple coût.
- Nouvelles exigences :Les consommateurs et les partenaires exigent désormais un haut niveau de sécurité, soutenu par la loi.
- Nouvelle perspective :La cybersécurité devient un produit différencié, un pilier stratégique et un facteur de compétitivité, car elle influence directement l'expérience client.

L'IA sécurisée comme argument de souveraineté

- Le label SecNumCloud de l'ANSSI permet de prouver objectivement la qualité d'une infrastructure et fait de la souveraineté des données un argument commercial, garantissant une protection contre l'ingérence d'autorités étrangères.
- **Exemples d'acteurs nationaux :**

    - Outscale (Dassault Systèmes) communique sur sa capacité à "opérer la transformation numérique avec le cloud souverain".
    - Mistral AI utilise l'argument de l' "IA souveraine".
    - Bleu (Capgemini/Orange) opère Microsoft Azure. Orange Business a migré 70 % de son infrastructure IT vers Bleu, valorisant sa maîtrise de la connectivité.
- Avantages de la labellisation :Localisation des données sur le territoire national, protection juridique renforcée et confiance accrue.
-

L'impact de l'Intelligence Artificielle (IA) générative sur la cybersécurité

L'IA générative est un facteur de transformation majeur, à la fois pour les attaquants et les défenseurs.

L'IA pour la défense des cyberattaques

- Principe de fonctionnement :Tout comme l'IA générative peut prédire le mot suivant dans une phrase, elle peut prédire l'étape suivante dans une cyberattaque.
- Détection améliorée :L'IA peut corréler des signaux faibles et non directement liés, "comblant les trous" pour révéler une attaque complexe en plusieurs étapes. Un analyste peut poser une question en langage naturel ("J'ai une machine qui se comporte bizarrement") et obtenir une analyse rapide des logs.
- Détection de falsifications :L'IA est utilisée pour détecter des "artefacts" dans des vidéos (deepfakes) ou des documents falsifiés.

L'IA pour les cyberattaques

- Une attaque sophistiquée qui prenait plusieurs semaines peut désormais être réalisée en quelques heures. Les attaquants contournent les sécurités des IA en découpant l'attaque en centaines de micro-tâches, chacune exécutée par un "agent" (une instance de l'IA). 90 % de l'attaque est automatisée.
- Le cas des failles "zero-day" :Avec l'IA, les hackers peuvent créer en quelques heures un logiciel pour exploiter une faille nouvellement révélée chez tous ceux qui n'ont pas encore appliqué le correctif.
- Inondation des communautés open source :L'IA génère un volume excessif de propositions (failles, corrections) qui "déborde le dispositif classique de gouvernance du code", créant une faiblesse majeure.

Le besoin de formation en IA sécurisée

Il existe un "vrai problème de formation" des développeurs. Il est possible de développer des modèles d'IA sur des données cryptées sans y accéder en clair,

mais cette pratique, courante en médecine, est peu connue dans le monde de la gestion.

L'Identité Numérique comme solution d'avenir

Romain Santini, Directeur de programme - identités numériques & eidas2 chez Docaposte, a présienté **eIDAS v2**, règlement européen qui modernise en profondeur la gestion de l'identité numérique. Il impose en effet un cadre harmonisé à l'échelle de l'Union Européenne, avec un *wallet* d'identité interopérable destiné à sécuriser l'authentification, les transactions et l'accès aux services en ligne. Les entreprises devront s'aligner sur ces exigences qui deviennent le socle des modèles économiques dématérialisés.

- Bilan de la première version d'eIDAS (2014) :Un "relatif constat d'échec"car l'objectif d'interopérabilité des identités numériques en Europe n'a pas été atteint. Le modèle était trop libertaire et les États n'étaient pas obligés de développer des solutions".

- **Les nouveautés d'eIDAS 2 : Le portefeuille d'identité numérique (wallet) :**
    - Partage de données sélectif : L'utilisateur pourra partager uniquement l'information nécessaire (prouver sa majorité sans révéler sa date de naissance, par exemple).

    - Sécurité et interopérabilité "by design" :La Commission imposera des spécifications communes pour que tous les portefeuilles européens fonctionnent de la même manière.

- **Calendrier et obligations :**
    - Décembre 2026 :Les États membres doivent rendre le portefeuille disponible pour leurs citoyens.
    - Décembre 2027 :Acceptation obligatoire par les services publics, les entreprises exigeant une authentification forte (banques) et les "très grandes plateformes en ligne" (Facebook, LinkedIn, etc.). L'acceptation est obligatoire, mais l'usage reste un choix pour l'utilisateur.

Les déclinaisons du concept de portefeuille

- Le portefeuille d'entreprise permettrait au représentant légal d'effectuer des démarches au nom de l'entreprise de manière sécurisée et interopérable à l'échelle européenne.
- Le portefeuille d'employé : Concept non réglementé mais logique, qui pourrait remplacer les badges d'accès et identifiants de connexion par une seule application mobile.

Exemples de systèmes d'identité numérique intégrés

- **Systèmes européens :**
    - BankID (Norvège/Suède) et Itsme (Benelux) : Systèmes créés par les banques, offrant une expérience transparente aux citoyens. Ils devront migrer vers le standard eIDAS 2.
- **Écosystèmes étatiques :**
    - Estonie et Inde :Exemples de systèmes hautement intégrés, vus non comme une contrainte mais comme un levier de croissance et d'efficacité. Le système estonien est si résilient que le gouvernement pourrait "redémarrer directement au Luxembourg" en cas d'invasion.
    - Système indien :Un site e-commerce n'a besoin que du numéro de portable de l'utilisateur et n'a jamais accès à ses coordonnées bancaires, qui sont gérées via des services étatiques.

Enjeux de souveraineté, de sécurité des données et d'usage

Concilier sécurité et simplicité d'utilisation

- Complexité perçue :Les solutions comme l'Identité Numérique de La Poste sont jugées "pas simples à mettre en œuvre", ce qui explique la persistance des mots de passe faibles.
- Relativiser la complexité :Comparé à l'alternative (se déplacer en agence, gérer des dizaines de mots de passe), l'usage de ces applications est en réalité plus simple et offre des bénéfices concrets.
- La promesse d'eIDAS 2 vise à rendre les choses "plus faciles" pour le citoyen, malgré une architecture sous-jacente complexe.
- Nécessité de standardisation : Il est suggéré de "forcer les utilisateurs" à adopter des interfaces simples et sécurisées pour sortir du modèle identifiant/mot de passe.

Sécurité des données chez les géants de la tech (exemple de Microsoft)

- Engagements contractuels :Microsoft s'engage contractuellement à ne pas accéder aux données en clair de ses clients. Les données sont chiffrées au repos et en transit, et les clients peuvent utiliser leurs propres clés.
- Le "Confidential Computing" :En collaboration avec Thales, cette technologie permet de chiffrer la donnée jusqu'à son traitement à l'intérieur même du processeur, la rendant inaccessible même pendant son utilisation.
- Évolution des algorithmes :La menace de l'ordinateur quantique est anticipée, et des travaux sont en cours avec l'ANSSI pour développer de nouveaux algorithmes. L'obsolescence des anciens algorithmes est un risque réel (ex: un disque dur sous Windows 10 avec une puce TPM 1.0 peut être déchiffré en moins d'une heure).

La conférence a mis uen lumière une tendance fondamentale : la cybersécurité n'est plus une simple fonction de support mais un pilier stratégique et un moteur d'innovation. L'avènement de l'IA générative instaure une nouvelle course à l'armement, où cette technologie est à la fois une arme redoutable pour les attaquants et un outil de défense indispensable. Un consensus se dégage sur le fait que la sécurité doit aller au-delà de la gestion des mots de passe pour englober la protection de toutes les données personnelles à travers des systèmes intégrés, comme le promet le portefeuille d'identité numérique européen (eIDAS 2). Cependant, la mise en œuvre de solutions à la fois sécurisées et simples pour l'utilisateur reste un défi majeur, exacerbé par les enjeux géopolitiques de souveraineté des données et les modèles économiques des géants de la tech. La discussion souligne la nécessité d'une prise de conscience politique forte et d'une stratégie claire pour naviguer entre les impératifs de sécurité, les réalités économiques et les standards technologiques mondiaux.