Un peu de bon sens cyber !

Un regard simple et actionnable pour dirigeants
pour assurer la protection des actifs les plus stratégiques du SI

noways.

C’est désormais chose connue, le risque cyber n’est pas théorique

Impact au niveau global

30% : hausse des attaques en 2023 portée par l’augmentation du nombre de ransomwares (+40%)[1]

~$3 millions : rançon moyenne en cas d’attaque par ransomware [2]

$42 milliards : coût total estimé des ransomwares en 2024 [3]

$265 milliards : coût que pourrait atteindre les ransomwares en 2031 [4]

Impact à l’échelle française

~50% : des entreprises ont constaté une attaque significative ou plus en 2023 [5]

210 jours : durée moyenne pour identifier une violation du SI par les entreprises [6]

~4 millions € : coût moyen d’une violation de données en France en 2023 ($4,17m) [6]

Performance des attaques [10]

+50% : taux de click sur du phishing ciblé par IA [7]

68% : attaques avec faille humaine comme point d’entrée (ingénierie sociale, phishing, …) [8]

+70% : des attaques parviennent à chiffrer les données [2]

~75% : des attaques n’utilisaient pas de logiciel malveillant. [9]

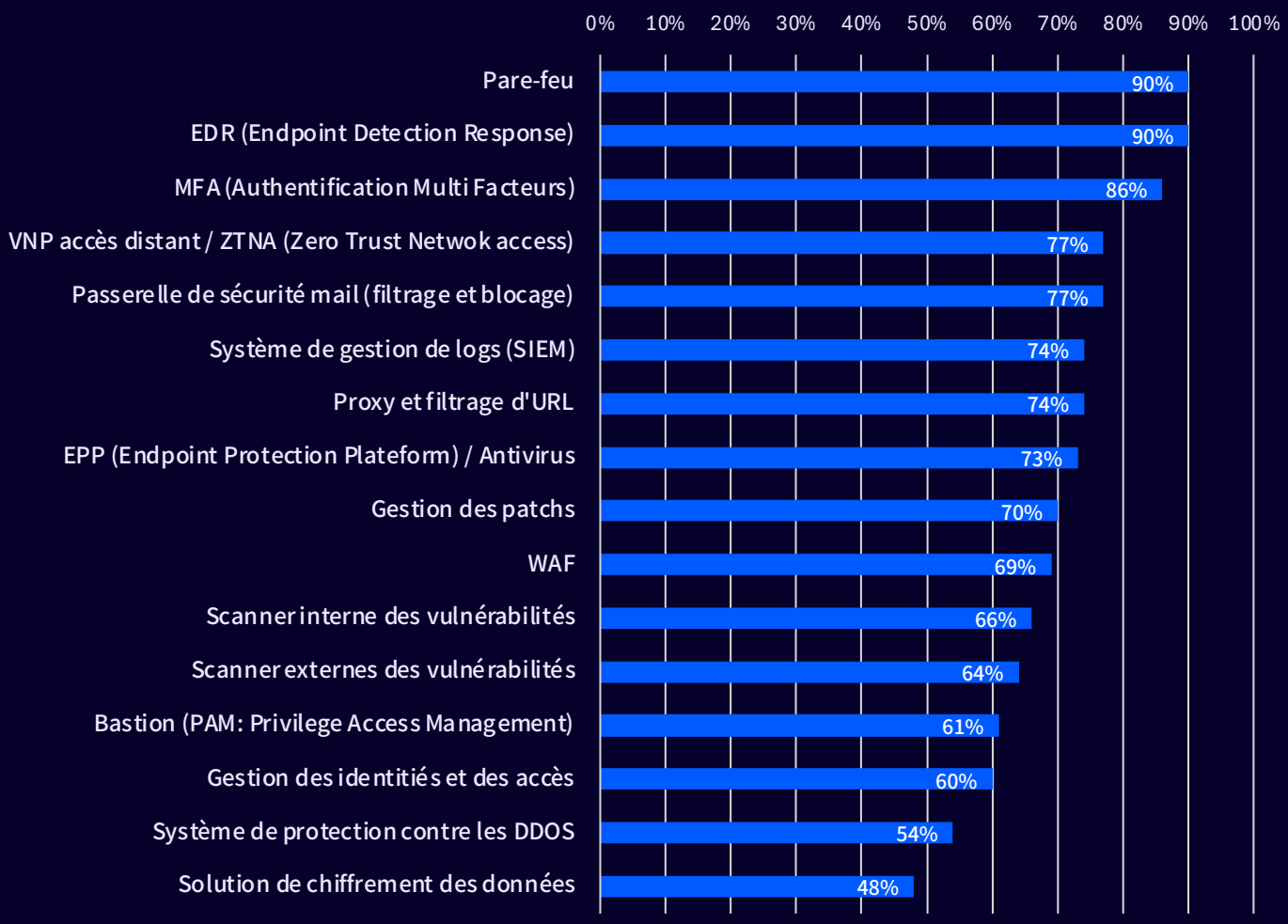
[1] European Union Agency for Cybersecurity, Threat landscape 2024
[2] Rapport Sophos sur l’état des Ransomwares 2024
[3] Etude Esentire - Cybercrime, Cost to the World
[4] Top 10 trends Cyber Security Ventures

[5] Baromètre du CESIN 2024
[6] Rapport IBM sur les coûts des violations de données

[7] Evaluating Large Language Models’ Capability to Launch Fully Automated Spear Phishing Campaign
[8] Etude Verizon Data Breach
[9] Crowdstrike : Global threat report 2024
[10] Données 2024

Pour s’en prémunir, de très nombreux moyens sont déjà déployés

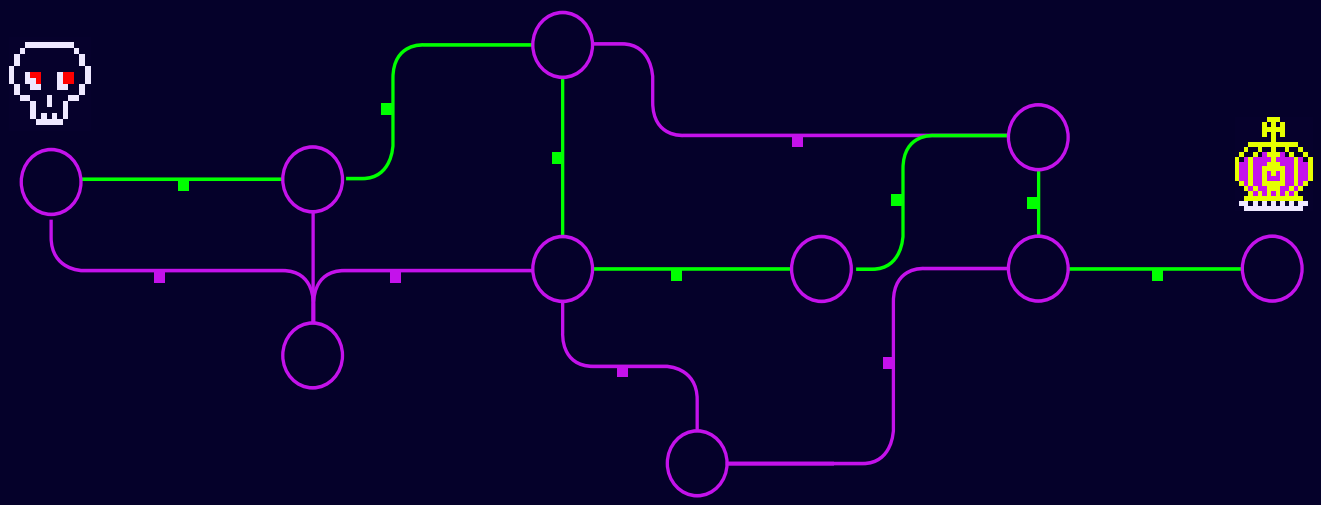
Taux de déploiement en moyenne dans les entreprises par type de solution



Malgré toutes ces solutions,
une question simple, mais essentielle, reste sans réponse

Source: Baromètre du CESIN 2024

“Savez-vous comment un attaquant peut naviguer dans votre réseau, de la surface vers vos actifs les plus précieux?”



Question au de toute cyberattaque sérieuse

Intrusion par la surface
Le pied dans la porte

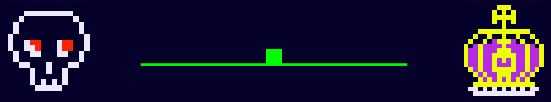
Un attaquant utilise une faiblesse, technologique et / ou humaine pour mettre un pied dans la porte. Il entre dans le SI.

Même si réduire sa surface exposée est crucial pour limiter les risques, un attaquant finira par réussir à s'introduire s'il y consacre assez de temps et d'efforts.

1

Mouvement latéral
La navigation dans le SI

2



L'attaquant se déplace dans le SI, de proche en proche, en utilisant des routes laissées ouvertes.

Comme l'attaquant joue des manques de cohérence des configurations en place, son comportement semble légitime.

Exécution
Actions malveillantes

3

Vols de données, compromission des opérations métiers, ransomwares…

L'attaquant est arrivé dans une zone sensible, il met en oeuvre ses intentions malveillantes

Même si détecté, il est trop tard.

Supprimer le mouvement latéral pour couper toute capacité d'attaque sévère

Contenir le risque ou le prévenir ?

D'un côté, l'intrusion est inévitable. Ne serait-ce que par les statistiques de phishing, il est clair qu'une campagne de qualité dans la durée créera une brèche. Des efforts sont bien évidemment nécessaires pour contrôler sa surface, réduire le niveau de risque et éviter d'être une cible trop aisée. Mais l'intrusion reste inévitable à terme.

D'un autre côté, lorsque les actions malveillantes sont exécutées, le mal est fait. Oui ! Il est évident que détecter au plus tôt l'activité suspecte et tenter de la bloquer est nécessaire. Mais c'est une posture d'endiguement, non de prévention structurelle.

Comment donc prévenir le risque ? En coupant structurellement tout risque de mouvement latéral.

Des solutions du marché apportent des premiers moyens d'action

- Permettant d'agir pour ouvrir / fermer des flux (e.g. CSPM, NSPM[1])
- Offrant des vérifications basées sur des standards et bonnes pratiques (e.g. CSPM, NSPM)
- Proposent une capacité de filtrage au niveau le plus fin - microsegmentation (e.g. ZTS [1])
- Couplant risque réseau avec d'autres vecteurs d'attaque (e.g. vol d'identité)

Un pilotage à l'aveugle, sans maitrise factuelle des risques

Le problème ? Aucune des catégories évoquées ci-dessus n'apporte la finesse de compréhension du réseau nécessaire pour répondre à la question clef : en l'état, savez-vous comment un attaquant peut naviguer dans votre réseau, de la surface vers vos actifs les plus précieux ?

Résultat, des couches de sécurité sont ajoutées par nécessité, mais le pilotage reste effectué à l'aveugle, sans maîtrise des options laissées à la disposition d'un intrus pour naviguer dans le SI.

Or, des innovations émergentes offrent une solution idéale

Un moyen pour revenir facilement aux fondamentaux, levant tous les freins structurels habituels, et fournissant les outils pour mettre en oeuvre des principes *de base* garantissant une sécurité efficace:

S'il n'y a pas de route, il n'y a pas de flux ...
S'il n'y a pas de flux, il n'y a pas d'attaque

[1] CSPM : Cloud Security Posture Management, NSPM: Network Security Policy Management, ZTS : Zero Trust Segmentation

Pour y arriver, un chemin semé d'embûches

Complexité croissante des infrastructures IT

Les ETI ont en moyenne 1000 à 1500 objets réseaux, ce qui génère des centaines de millions de routes potentielles que des attaquants pourraient exploiter.

Les réseaux de plus en plus hybrides, combinant des serveurs on-premise et des ressources cloud, compliquent davantage la gestion et le contrôle du SI, par la multiplication et diversité des technologies à intégrer et à maitriser.

Gouvernance et responsabilité dans l'organisations IT

A la croisée de l'architecture, des opérations d'infrastructure et de la cyber, le sujet est victime du manque de clarté sur les responsabilités, la gouvernance et le budget.

Situation aggravée par des équipes IT saturées et ne pouvant plus traiter de nouveaux sujets. En 2023, 73% des responsables IT estiment que leur équipes sont surchargées et ne peuvent accomplir leur mission[1].

Difficulté d'accès aux ressources et compétences

60% des entreprises françaises rencontrent des difficultés pour recruter des talents IT qualifiés, notamment dans les domaines de la cyber, des architectures et du cloud [2].

La pénurie de talents a entraîné une forte augmentation des coûts pour accéder à cette expertise. A titre d'exemple, les experts en sécurité cloud voient leurs salaires augmenter de 20 à 30% par rapport aux profils traditionnels.

Un outillage inadapté

Les audits et tests d'intrusion sont ponctuels et manuels, de fait long, coûteux avec un périmètre d'analyse restreint. Ces résultats, statiques, ne sont qu'une photo à un instant *t* du SI.

La majorité des outils de contrôle du réseau nécessitent l'installation d'agents sur chaque PC et serveur, ou l'installation de sondes pour analyser les flux de production. Ce qui n'est pas sans risque pour les opérations métiers[3]. D'autres solutions reposent sur un contrôle des règles de sécurité en place, à base de vérifications statiques déclinant différentes normes (e.g. PCI-DSS) et bonnes pratiques. Approche *top-down* sans compréhension des spécificités propres d'un SI.

[1] Etude IDC
[2] Rapport «European ICT Skills Survey» du Cepis (Council of European Professional Informatics Societies)
[3] Cf articles sur le bug Crowdstrike qui a provoqué un blocage mondial

Parer ces obstacles avec un focus sur 3 actions ...

I Maitriser son réseau

Connaitre à tout moment l'état exact du réseau, tel qu'il est réellement configuré, même si cela diffère du design ou des politiques initiales (résultat d'actions quotidiennes).

Comprendre les flux qui passent, ceux qui ne passent pas, pour diagnostiquer finement et agir avec précision.

II Prioriser les éléments critiques du SI

Concentrer les efforts sur les applicatifs critiques dont la résilience et l'étanchéité sont indispensables au business.

A tout vouloir sécuriser, on ne sécurise rien…

III Assurer de la pérennité dans le temps

Tous les Systèmes d'Information vivent, tous les réseaux évoluent constamment. Le moindre changement non maitrisé peut créer des vulnérabilités exploitables par des attaquants.

Les audits ad-hoc ne sont pas suffisants pour assurer une sécurité des actifs critiques .

… et s’appuyant sur deux innovations émergentes pour agir sans peine

Le jumeau numérique du réseau

Réplique virtuelle du réseau qui capture et cartographie l’ensemble de ses éléments (serveurs, routeurs, pare-feu, etc.) mais aussi leur état et configuration pour modéliser dans un environnement numérique le comportement exact du réseau en production.

Cela permet une compréhension complète et détaillée du réseau. Ainsi que la conduite de diagnostiques continus sans impact sur la production.

Historiquement, des agents ou sondes installés dans le réseau étaient nécessaires pour obtenir cette compréhension. Or, ces solutions sont complexes à manager et coûteuses ; impactent la performance du réseau et sont non sans risques pour les opérations métiers.

Aujourd'hui, il est désormais possible de créer facilement des jumeaux numériques, offrant ainsi une compréhension sans précédent du réseau sans ces inconvénients.

Les algorithmes d’analyse avancée [1]

De nouvelles approches algorithmiques permettent de simuler le comportement des attaquants au sein du réseau, pour identifier les faiblesses d’architectures, les incohérences entre les différentes règles de sécurité … et comprendre ainsi comment un attaquant peut déjouer les contrôles en place pour naviguer jusqu’à des cibles de forte valeur.

En intégrant ces algorithmes aux jumeaux numériques, les organisations IT sont désormais capables de repérer rapidement et précisément les vulnérabilités du réseau. Cela permet d'agir proactivement pour les corriger avant qu'elles ne soient exploitées par des attaquants.

[1] Catégorie appelée par Gartner ASCA - Automated Security Control Assessment

En synthèse

La menace cyber est réelle et croissante

En 2023, 50% des entreprises européennes ont été attaquées, avec une hausse de 30% des cyberattaques.

Les ransomwares continuent de faire mal avec des rançons moyennes de $3m et un coût global de $42 milliards en 2024. En France, le coût moyen d'une violation de donnée a un impact d'environ 4m d'euros, avec +200 jours pour l'identifier et +70 jours pour la contenir.

La prévention du mouvement latéral reste un angle mort

Les entreprises font face à une complexité accrue des infrastructures IT (serveurs locaux + cloud), à un manque de compétences en cybersécurité, et à des outils souvent inadaptés.

Malgré l'usage de nombreuses technologies, les attaquants arrivent à pénétrer le SI. Une fois rentré, le mouvement latéral des attaquants reste difficile à bloquer efficacement.

Une des causes principales: il n'y a pas de maitrise du réseau pour savoir facilement et à tout instant quelles sont les routes réseaux que peut prendre un attaquant pour naviguer jusqu'à des cibles de forte valeur.

Des innovations technologiques émergent pour palier à ce manque

Alors qu'aucune catégorie de produit claire n'existe pour assurer une architecture sécurisée, deux innovations émergentes permettent d'agir efficacement:

- le jumeau numérique du réseau, qui offre une compréhension complète du réseau, à tout instant et sans effort
- les algorithmes d'analyse avancée[1], simulant le comportement des attaquants, pour cibler les actions de sécurisation des actifs à plus forte valeur

Une nouvelle approche pour une réponse *réellement* efficace

Cette approche permet aux équipes IT d'assurer une architecture réseau sécurisée, sans charge accrue, en continu et à l'échelle de l'entreprise.

Agissant au niveau le plus élémentaire (un flux passe ou non ...), cette combinaison apporte une solution réellement efficace pour protéger les SI et accroître leur résilience face aux attaques.

[1] Catégorie appelée par Gartner ASCA - Automated Security Control Assessment

A propos

noways est une entreprise française innovante, fondée en 2023 et basée à Paris.

Notre mission :
Permettre à nos clients de reprendre le contrôle de leur réseau pour prévenir tout temps d'arrêt, de manière simple, pro-active, et efficace.

Pour atteindre cet objectif, **noways** propose une plateforme logicielle clé en main, destinée aux entreprises et organismes publics, leur permettant de bâtir, maintenir et contrôler une architecture réseau fiable et sécurisée.

Unique en son genre, la plateforme **noways** combine ensemble deux innovations majeures :

- Un **jumeau numérique du réseau** : modèle virtuel dynamique du réseau (Cloud / On-premise), construit automatiquement et offrant une compréhension complète de l'infrastructure réseau et de ses flux.
- Des **algorithmes d'analyse centrés métiers** : des agents pouvant simuler le comportement d'attaquants, mais aussi l'ensemble des flux légitimes, pour

  (i) anticiper en continu et à l'échelle du SI comment un intru peut naviguer malicieusement vers les actifs les plus précieux ;

  (ii) anticiper en continu et à l'échelle du SI l'impact de tout changement sur le réseau ;

  (iii) assurer en continu et à l'échelle du SI la continuité de service en bloquant structurellement les routes à risque avant qu'une attaque ne survienne et en évitant des effets de bord sur les flux métiers.

Avec **noways**, nos clients simplifient la gestion de leur sécurité réseau, sans effort, sans agent, sans risque.

Contacts:
Louis Vatier, CEO - louis@noways.io
Salim Moulay Rchid, COO - salim@noways.io

noways.

Reprenez le contrôle de la sécurité de votre réseau