Veille technologique et Juridique

L’utilisation de l’achitecture Zero Trust

Sommaire :

Introduction :

Contexte général :

Les technologies actuelles sont en constante évolution, les entreprises telles que sopra steria s'adaptent tandis que cyber menaces sur ces entreprises sont plus fréquentes menant à un besoin d'améliorer la sécurité et les technologies en général.

Contexte professionnel :

Je suis helpdesk a soprasteria et mon travail consiste à aider les utilisateurs à déposer leurs factures sur la plateforme publique Chorus Pro ou l'utilisattion du site par le biais d'un tchat ou d'un outil de ticketing. A sopra steria la cybersécurité est un enjeux majeur car les données qui y circulent ne sont pas des données qui peuvent être transmis à l'extérieur de l'entreprise.
Je traite donc des données plus sensibles nécessitant une haute sécurité, les informations de facturation sur les utilisateurs a ma disposition par exemple doivent être protégé et mes propres accès à mon poste de travail jusqu'au site dispose de plusieurs sécurité comme des méthodes d'authentification.C'est dans ce contexte que l'architecture zero trust est utile.

Raison de la veille :

J'ai donc choisi ce sujet de veille technologique car l'architecture zero trust En lien direct avec mon environnement de travail.La cyber sécurité est un enjeu majeur face au cyberattaque ainsi que la gestion des acces, Zero trust permet de travailler plus en sécurité, limite les dégâts liés aux cyberattaques, facilite la conformité réglementaire des données sensibles et améliore l'expérience des employés avec des méthodes de sécurités plus flexibles. Ce sujet est présent partout car il y souvent une gestion des données sensibles. C'est donc un sujet au cœur de de l'informatique qui aura pour conséquence une évolution.

Problématique :

Pourquoi l'utilisation de zero trust serait bénéfique pour sopra steria et ses enjeux lié à la sécurité et comment ce modèle peut améliorer la sécurité ?

Quel est la meilleure méthode d'application du modèle zero trust ?

Concept Zéro Trust :

Si on regarde comment la sécurité informatique a évolué, on se rend vite compte que les vieilles méthodes où on protégeait tout avec juste un pare-feu, c'est clairement dépassé. Dès qu'Internet, le cloud et le travail à distance se sont démocratisés, ça ne marchait plus pareil. Des groupes comme Jericho Forum ont commencé à remettre ça en question dans les années 2000. Mais le vrai tournant, c'est en 2010 avec un expert, John Kindervag (Forrester), qui a vraiment posé les bases du Zero Trust : , il faut tout vérifier, tout le temps, même pour les personnes ou les machines qu'on connaît déjà.

Avantages principaux :
-Réduction du risque : les attaques informatiques sont plus difficilement réalisables, car le "mouvement latéral" entre systèmes est limité.

-Meilleure gestion des accès : chaque compte, chaque permission est vérifiée, empêchant le vol de données sensibles.

-Adapté aux environnements modernes : idéale pour les entreprises gérant plusieurs clients, comme Sopra Steria, qui doit sécuriser des plateformes critiques.

-Conformité : le Zero Trust aide à respecter les normes (ANSSI, NIS2, RGPD), très importantes dans le secteur public et les grandes entreprises.

Inconvénients :
-Mise en œuvre complexe : il faut revoir l'organisation du réseau, installer de nouveaux outils (IAM, ZTNA) et former le personnel.

'-Coûts initiaux : achat d'outils et adaptation des infrastructures.

-Impact sur les utilisateurs : authentifications fréquentes et nouveaux processus qui peuvent ralentir l'activité au départ.

Les versions et l'évolution du Zero Trust :

Depuis sa naissance en 2010, le Zero Trust s'est beaucoup transformé. On distingue désormais plusieurs architectures, évoluant selon les recommandations d'organismes comme le NIST et la CISA. Le modèle de maturité CISA, révisé en 2023, propose quatre niveaux : traditionnel, initial, avancé et optimal, chacun nécessitant davantage de sophistication dans la protection et la gestion des accès. Les mises à jour officielles sont fréquentes, pour intégrer de nouveaux usages (cloud, mobilité) et répondre aux menaces émergentes.
Les solutions Zero Trust évoluent aussi fonctionnellement. Par exemple, les produits intègrent de plus en plus l'IA pour optimiser la détection des menaces et l'ajustement des politiques en temps réel. L'adoption du multifacteur sans mot de passe ou la gestion dynamique des droits sont des évolutions récentes et marquantes.

Le marché propose divers outils Zero Trust : Palo Alto Prisma Access, Okta, Citrix Secure Private Access, Check Point SASE, Sophos, Cloudflare Access, Zscaler, IBM… Chacun offre une protection plus ou moins complète selon les besoins : micro-segmentation, gestion des identités, surveillance réseau et compatibilité cloud. Les critères de choix sont : couverture fonctionnelle, facilité d'intégration, support, ergonomie et conformité NIS2/ANSSI

Solution	Couverture	Points forts	Note sur 5	Coût annuel
Palo Alto Prisma	Complète	Micro-segmentation, cloud ready	4,5	35k €
Okta	Complète	SSO, MFA, gestion identité	4,5	25k €
Zscaler	Complète	Accès réseau, cloud natif	5	40k €
Citrix SPA	Partielle	MFA, contrôle accès, hybride	3,5	18k €
Cloudflare	Complète	Accès basé identité et contexte	5	36k €

https://www.sentinelone.com/fr/cybersecurity-101/identity-security/zero-trust-vendors/

https://foxeet.fr/contenu/top-10-solutions-zero-trust-nis2

Coûts à prévoir :

Le coût du Zero Trust dépasse l'achat des logiciels. Il faut intégrer :
-Le temps des équipes (cartographie, classification, migration)
-La formation des utilisateurs et du support
-La gestion du changement organisationnel

Le principal obstacle à l’adoption reste le coût global (licences, services, adaptation interne), surtout au début. Mais une fois en place, une entreprise observe des économies : réduction des incidents, surveillance simplifiée, meilleure productivité… utilisation Zero Trust pour valoriser leur expertise et proposer des services à forte valeur ajoutée, ce qui justifie l’investissement sur le long terme.