18 /3/2024

Introduction du devoir :

La prévision dans la conformité en matière de cybersécurité revêt une importance cruciale pour les organisations, car elle permet d'anticiper et de se préparer aux menaces potentielles, de se conformer aux réglementations en vigueur et de réduire les risques liés à la sécurité des données et des identités. Les objectifs de cette mission sont de prédire les évolutions des menaces cybernétiques, d'identifier les vulnérabilités potentielles et de mettre en place des mesures proactives pour se conformer aux normes de sécurité et de protection des données. Les attentes de cette mission incluent la capacité à anticiper les tendances des cybermenaces, à évaluer les risques potentiels et à élaborer des stratégies de conformité efficaces pour protéger les données et les identités contre les attaques cybernétiques.

X-Force Threat Intelligence Index 2024 page 3, 4 et 8.

Méthodologie :

La démarche que nous avons suivi :

- Identifier les émetteurs des documents : état français, sociétés leader en solutions cyber sécurité, américaines, israélo-américaine, des sociétés de conseil comme Wavestone, protecteurs des droits individuels, la CNIL.
- Identifier les types de documents : rapport, projections, enquête auprès des entreprises, une interview. J'ai exclu l'enquête cybersécurité de CESIN.

Résultats:

Présentez vos résultats principaux. Mettez en évidence les tendances prédites en matière de cybersécurité pour 2024 et leur impact attendu sur les normes de conformité actuelles ou à venir.

Les défis émergents en matière de cybersécurité, tels que les attaques automatisées dans les environnements cloud, la manipulation de données pour compromettre les modèles d'IA et ML, les menaces liées à l'IA générative, les attaques sur les chaînes logicielles et les risques associés aux blockchains privées, auront un impact significatif sur les normes de conformité actuelles et à venir.

Ces défis nécessiteront une adaptation des normes de conformité pour inclure des mesures de sécurité préventives plus rigoureuses, telles que la validation et l'authentification approfondies des ensembles de données d'entraînement, ainsi que des contrôles de sécurité renforcés pour les environnements cloud et les chaînes logicielles. De plus, les normes de conformité devront probablement intégrer des directives spécifiques pour la protection des modèles d'IA et ML contre la manipulation de données, ainsi que des exigences de sécurité pour les blockchains privées.

En résumé, les défis émergents en matière de cybersécurité auront un impact sur l'évolution des normes de conformité, les poussant à intégrer des mesures de sécurité avancées pour faire face aux menaces cybernétiques émergentes.
Critical_Scalability-Trend-Mico Sécurity predictions for 2024 Page 3 4 10

Le rapport propose plusieurs conseils pour réduire le risque d'attaques liées à la collecte d'informations d'identification. Il recommande le déploiement d'outils EDR sur tous les serveurs et postes de travail pour détecter les logiciels malveillants, les comportements anormaux et les attaques d'exfiltration de données. De plus, il suggère de renforcer les pratiques de gestion des informations d'identification en mettant en œuvre des politiques d'authentification multi-facteur, des mots de passe sécurisés et des configurations système renforcées pour rendre l'accès aux informations d'identification plus difficile. En outre, le rapport encourage l'utilisation de l'IA pour traiter jusqu'à 85 % des alertes et bénéficier de services de détection et de réponse aux menaces 7 jours sur 7. Enfin, il recommande l'utilisation de renseignements sur les menaces pour identifier les principales opportunités permettant d'atténuer les menaces

nouvelles et émergentes des pirates informatiques cherchant à dérober des informations d'identification.
Page
X-Force Threat Intelligence Index 2024 page 3, 7 et 8

Quels sont les principaux défis en matière de cybersécurité attendus en 2024 selon le document ?
Selon le document, les principaux défis en matière de cybersécurité attendus en 2024 comprennent :

1. Les menaces liées aux environnements cloud, y compris les attaques automatisées, les défis de défense contre les attaques cloud-native et les risques de configurations erronées.
2. La protection des modèles d'apprentissage automatique (ML) contre la manipulation de données, avec un accent sur la validation et l'authentification approfondies des ensembles de données d'entraînement.
3. Les risques associés à l'utilisation de l'intelligence artificielle générative (Generative AI), y compris les deepfakes, les clones vocaux et les attaques ciblées.
4. Les menaces potentielles sur les chaînes logicielles, y compris les attaques sur les logiciels couramment utilisés et les risques de compromission des chaînes logicielles.
5. Les défis liés à la sécurité des blockchains privées, notamment les risques d'extorsion et de compromission des données.

En outre, le document met en évidence les menaces potentielles liées aux tensions géopolitiques actuelles, telles que les cyberattaques politiquement motivées et les campagnes de désinformation orchestrées à l'aide d'outils et de plateformes alimentés par l'IA.
Critical_Scalability-Trend-Mico Sécurity predictions for 2024 Page

Conclusion:

1.**Résumé des Principales Découvertes :**

Les principales découvertes telles que révélées par Check Point Research (CPR) mettent en évidence l'évolution des attaques cybercriminelles avec l'augmentation des cyberattaques mondiales, l'évolution des ransomwares, **l'utilisation croissante de l'intelligence artificielle (IA) par les cybercriminels, et les prévisions concernant les attaques sur le cloud, la chaîne d'approvisionnement et les infrastructures critiques.** Il souligne également l'importance croissante de la cyber-assurance, les attaques menées par des États-nations et le **hacktivisme**, ainsi que l'exploitation

croissante de la technologie **deepfake** et les attaques de phishing. En outre, le document met en lumière les prévisions concernant les ransomwares, mettant en garde contre l'utilisation avancée de l'IA par les attaquants, l'adoption de tactiques plus discrètes et la nécessité pour les organisations de renforcer leurs mesures de cybersécurité pour faire face à ces évolutions. Enfin, le document souligne l'importance pour les organisations d'adapter leurs mesures de cybersécurité pour faire face à l'expansion des vecteurs d'attaque.

Into the Cyber Abyss Check Points Riveting 2024 Predictions Reveal a Storm of AI

2. **Implications pour la Conformité en Cybersécurité :**

Les défis émergents en matière de cybersécurité, tels que les attaques automatisées dans les environnements cloud, la manipulation de données pour compromettre les modèles d'IA et ML, les menaces liées à l'IA générative, les attaques sur les chaînes logicielles et les risques associés aux blockchains privées, auront un impact significatif sur les normes de conformité actuelles et à venir.

Ces défis nécessiteront une adaptation des normes de conformité pour inclure des mesures de sécurité préventives plus rigoureuses, telles que la validation et l'authentification approfondies des ensembles de données d'entraînement, ainsi que des contrôles de sécurité renforcés pour les environnements cloud et les chaînes logicielles. De plus, les normes de conformité devront probablement intégrer des directives spécifiques pour la protection des modèles d'IA et ML contre la manipulation de données, ainsi que des exigences de sécurité pour les blockchains privées.

En résumé, les défis émergents en matière de cybersécurité auront un impact sur l'évolution des normes de conformité, les poussant à intégrer des mesures de sécurité avancées pour faire face aux menaces cybernétiques émergentes.

Critical_Scalability-Trend-Mico Sécurity predictions for 2024 Page 3, 4 et 10

3. **Recommandations Stratégiques (1 à 2 paragraphes) :**

1. Fournissez des recommandations pratiques pour les organisations, les décideurs politiques ou les professionnels de la cybersécurité, basées sur les tendances prévues et les implications en matière de conformité. Celles-ci devraient offrir des orientations sur la manière de se préparer et de s'adapter aux changements anticipés dans le paysage de la cybersécurité.

4. **Réflexion sur le Processus de Recherche (1 paragraphe) :**

1. Réfléchissez au processus de recherche, en reconnaissant les défis rencontrés ou les limitations observées pendant le devoir. Cela peut inclure des domaines où les informations étaient rares, les prédictions particulièrement incertaines, ou les leçons personnelles tirées.

5. **Directions pour les Recherches Futures (1 paragraphe) :**

1. Suggérez des domaines pour des recherches futures ou un suivi qui pourraient fournir des informations supplémentaires ou clarifier les incertitudes dans les prédictions en matière de cybersécurité. Cela encourage un engagement continu avec le sujet et reconnaît la nature constamment évolutive du domaine.

6. **Conclusion :**

Les responsables de la sécurité des systèmes d'information (RSSI ; en anglais, Chief information security officer ou CISO) doivent s'assurer que leurs opérations sont en conformité au-delà des certifications ISO ou des cadres NIST, en tenant compte des risques liés aux silos, migrations et changements. De plus, ils doivent se concentrer sur la consolidation des outils de sécurité pour améliorer l'efficacité et réduire la complexité. Enfin, ils doivent démontrer comment leurs demandes en matière de sécurité sont liées aux impératifs commerciaux et les bénéfices financiers ou les risques que chaque demande présente.

L'intelligence artificielle présente dans les plateformes de protection des postes de travail et de surveillance de l'infrastructure pour ajouter de la valeur, de l'efficacité, des performances et de la protection.

c'est un écosystème complet de partenaires que nous devons gérer à l'échelle mondiale.

Pour faire face à l'expansion des vecteurs d'attaque. de cybersécurité,

Cela implique l'adaptation, la collaboration et de transformation des partenaires.

Collaborer avec de nouveaux acteurs pour renforcer sa sécurité

Résilience : un enjeu majeur

La résilience opérationnelle est devenue une priorité ces dernières années, avec de **nouvelles réglementations** comme DORA (*Digital Operational Resilience Act*) pour le secteur financier, NIS2 (*Network and Information Systems Directive*) et le futur CRA (*Cyber Resilience Act*). Malgré des investissements croissants, la maturité en la matière reste faible avec des disparités significatives entre les organisations.

Radar du RSSI

Gestion des tiers : miser sur le collectif

Les attaques par le biais de tiers se sont multipliées en 2023. Les dernières en date touchant **Boeing, ICBC et DP World** soulignent la complexité de la gestion des tiers. La multitude de partenaires, fournisseurs et sous-traitants d'une organisation (et ses filiales !) fait de la gestion des tiers un véritable casse-tête pour les équipes cybersécurité.

Là encore, la **réglementation**, en particulier le chapitre V de DORA, appelle un contrôle accru. Pour répondre aux exigences du régulateur, il faudra évaluer les risques liés au tiers, élaborer des clauses spécifiques dans les contrats, et formaliser une stratégie de décontractualisation rapide (*stressed exit*).

Une gestion efficace des tiers ne peut pas reposer uniquement sur les équipes sécurité. **Tous les départements** doivent être impliqués : IT, achats, métiers… Une plateforme d'évaluation des tiers, accessible à tous, peut être une manière efficace de les engager.

Il faudra également impliquer vos tiers les plus critiques dans des **exercices de crise joints**. Cette préparation commune, encore trop rare, permet pourtant des apprentissages des deux côtés.

Enfin, une collaboration avec les **acteurs du même secteur** est cruciale pour protéger les éléments vitaux du marché. C'est particulièrement vrai pour les tiers qui ne peuvent être ré internalisés (par exemple : les grandes plateformes Cloud), ou lorsqu'aucune alternative n'existe pour le marché (par exemple : SWIFT).

La gestion des tiers, c'est gérer les risques de milliers, voire de dizaines de milliers, d'entités. C'est un travail majeur qui devra **se faire dans la durée !**

Radar du RSSI

RSSI : une fonction en pleine mutation

Face aux défis actuels, le rôle du RSSI (Responsable de la Sécurité des Systèmes d'Information) évolue pour intégrer de nouvelles compétences.

Radar du RSSI

En parallèle, l'avènement des **ordinateurs quantiques** incarne une menace grandissante. Bien que leur pic d'impact soit prévu entre 2030 et 2033, des signaux

d'alerte se manifestent déjà. Il faut donc réfléchir dès maintenant aux données sensibles qui devront rester confidentielles pendant au moins une décennie.

Trois étapes clés s'imposent dans la **transition vers le post-quantique**.

1. Identifier les données sensibles, en comprenant leur nature et leur importance stratégique, afin de prioriser la migration.
2. Analyser en profondeur les systèmes de chiffrement actuels, qu'ils soient commerciaux ou *open source*.
3. Adopter des solutions de chiffrement post-quantique, même imparfaites, pour tester et ajuster en continu.

A ce stade, une **stratégie de double chiffrement**, combinant méthodes traditionnelles et post-quantiques, offre une sécurité multicouche adaptée aux défis actuels et futurs.

Cybersécurité durable : quelles responsabilités pour les équipes ?

Dans un contexte d'urgence climatique, les équipes de cybersécurité doivent prendre leur part de responsabilité et adopter des pratiques durables, au-delà du *Green IT*. En effet le RSSI ayant la main sur les politiques de sécurité, il peut clairement les faire évoluer pour préconiser des mesures de sécurité moins consommatrices sans pour autant augmenter le niveau de risque.

Cela commence par **évaluer l'impact environnemental des mesures de sécurité**. Des outils existent pour mesurer les émissions de gaz à effet de serre des infrastructures (tant sur site que *Cloud*) et des *endpoints*. Cette première étape permet d'identifier les dispositifs les plus polluants au sein de l'organisation.

L'objectif est ensuite de **réduire les émissions sans compromettre significativement le niveau de sécurité**, c'est-à-dire sans toucher aux mesures critiques.

Des premiers travaux permettant de répondre opérationnellement à ce sujet seront publiés début 2024, restez à l'écoute !

2024… et après ? Préparer l'avenir !

Pénuries de talents cyber : des ressources à trouver en interne

Radar du RSSI