Business
Magazine

U & US

By Telindus

Air Gap
Un rempart contre la corruption des sauvegardes

Sécurité dans le cloud
Un enjeu sous-estimé

Smart Protection
Préalable et prolongement de la sécurité informatique

More inside

#12

CYBERSÉCURITÉ

ANTICIPER LES RISQUES ET RENFORCER SA SÉCURITÉ POUR SE PRÉPARER AUX NOUVEAUX DÉFIS NUMÉRIQUES

U&US #12

Chers amis, clients et partenaires,

Cette 12ème édition de notre magazine U&US est dédiée à la cybersécurité.

Dans un monde de plus en plus touché par les cyberattaques - toujours plus sophistiquées - les entreprises doivent relever des défis en matière de cybersécurité et faire preuve de réactivité.

Il est parfois difficile de s'y retrouver lorsqu'il s'agit de choisir la solution la plus adaptée en cybersécurité. Cette édition spéciale vous permettra de mieux comprendre, appréhender et surtout utiliser ces nouvelles solutions pour renforcer au maximum votre sécurité.

Au fil des pages, vous découvrirez pourquoi il est important de bien protéger vos données, votre cloud, vos bâtiments ou même vos infrastructures.

De l'élaboration d'une stratégie adaptée à la mise en pratique de celle-ci, vous bénéficierez également de tous les éléments clés pour réagir en cas d'attaque.

En vous souhaitant une excellente lecture,

GÉRARD HOFFMANN
CEO, Proximus Luxembourg

SOM-MAIRE

U&US #12

PROXIMUS LUXEMBOURG S.A.
18, rue du Puits Romain
Z.A. Bourmicht 8070 Bertrange
Tél :+352 450 915-1

GESTION ÉDITORIALE
Michaël Renotte

CONCEPTION GRAPHIQUE
Deuux

POUR ÉCRIRE À LA RÉDACTION
marketing@telindus.lu

@ telindustelecom
/Telindus-luxembourg
/Telindus_lu

À LA UNE

Gouvernance Risk Compliance : la solution adaptée pour une bonne conformité

RGPD, NIS2, DORA, CRA, CER, ... tant d'acronymes pour autant de challenges régulatoires. Le prochain rendez-vous majeur à ne pas manquer est celui de la NIS2. Cependant, toutes les entreprises ne se sentent pas forcément concernées. Dans ce cas, Telindus peut vous aider avec cette nouvelle directive.

Malgré la multiplicité et complexité de ces réglementations, il est important de contribuer à la sécurité globale de l'écosystème et de la société. La sécurité et la conformité ne s'improvisent pas mais se préparent et s'anticipent.

La solution Gouvernance Risk Compliance de Telindus permet de gérer les risques notamment en rassurant les entreprises de leur bonne conformité aux nouvelles réglementations.

L'AIR GAP

UN REMPART CONTRE LA CORRUPTION DES SAUVEGARDES

Les solutions Air Gap permettent de protéger les sauvegardes d'attaques ou de manipulations malveillantes. Ces sauvegardes protégées sont conservées hors du réseau, inatteignables, inaltérables et invisibles pour un attaquant ou un administrateur malveillant.

"Un Air Gap est une zone étanche, complètement déconnectée de l'environnement de production. Elle prélève les informations déposées dans un premier passage pour les analyser d'un point de vue sécurité et comportemental ensuite les données saines sont transmises dans la zone isolée", explique Olivier Bertin, Department Manager chez Telindus. "En réalité", dit-il, "la solution de sauvegarde que les entreprises utilisent est bel et bien une application de production. Celle-ci doit en effet être en mesure de capter tous les changements quotidiens et de restaurer immédiatement les fichiers et les éléments nécessaires au bon fonctionnement de l'entreprise en cas de besoin ou, en cas d'incident. Il en résulte que cette solution de sauvegarde est tout aussi critique que les applications de production standard".

L'APPROCHE DE TELINDUS : L'AIR GAP LOGIQUE

Le concept d'Air Gap repose sur une séparation physique ou logique entre un système informatique et tout autre réseau ou dispositif externe. Cette isolation garantit qu'aucune connexion ne peut être établie entre le système protégé et le reste du réseau. Un Air Gap physique introduit cependant une complexité considérable dans les processus de backup: gestion manuelle des sauvegardes, difficulté à appliquer les mises à jour, délai supplémentaire pour la restauration des données et de récupération des capacités de production, etc.

L'alternative consiste à mettre en place une approche d'Air Gap basée sur une isolation logique et organisationnelle plutôt que sur une isolation physique également connue sous le nom d'Air Gap virtuel ou Air Gap logique. " Plutôt que de déconnecter physiquement les systèmes, cette approche repose sur des méthodes de sécurité avancées pour établir une séparation stricte entre les systèmes de sauvegarde et le réseau principal. C'est ce type de solution que nous préconisons. ". L'approche de Telindus en matière d'Air Gap comporte deux volets.

CAPITALISER SUR LE SYSTÈME DE SAUVEGARDE EXISTANT

Une première solution consiste à capitaliser sur le système de stockage des données et de sauvegarde que l'entreprise exploite déjà. "Pour éviter un changement majeur ou l'obligation d'acquérir des compétences supplémentaires, nous mettons en place un "repository" dans lequel seront versés les backups en parallèle de la solution de sauvegarde existante", explique Olivier Bertin.

U-FLEX ET BACKUP AS A SERVICE

La seconde solution repose non pas sur le système de backup existant mais sur une nouvelle installation basée sur un équipement dédié ou sur une solution de Backup-as-a-Service (BaaS). " Telindus dispose d'une plateforme BaaS capable de télécharger les données sensibles d'une entreprise et de les mettre à l'abri isolé de l'environnement de production. Notre plateforme U-Flex, la plateforme d'externalisation informatique privée et réglementée, basée au Luxembourg et gérée par nos propres soins, se prête particulièrement bien aux applications de Backup-as-a-Service, de production et de reprise d'activités. " explique Olivier Bertin. La plateforme peut être complétée avec une offre de Managed Services qui permet au client de se concentrer sur ses activités fondamentales en confiant la gestion de sa solution de sauvegarde à nos équipes.

AU CŒUR DE LA CYBER-RÉSILIENCE

L'objectif de l'Air Gap est double, d'une part il analyse les données afin de s'assurer que les changements sur les informations déposées soient cohérents, en adéquation avec les activités régulières de l'entreprise et qu'aucun malware n'y soit intégré.

D'autre part il consiste à sécuriser des services vitaux qui ont été clairement identifiés dans le cadre d'une procédure d'évaluation des risques. Les services jugés critiques sont ensuite intégrés à la solution d'Air Gap afin d'assurer leur protection et leur rétablissement prioritaire en cas de besoin. C'est pourquoi son intégration relève de la gouvernance de la cyber-résilience.

"Toutes les organisations doivent mettre en œuvre une stratégie de cyber-résilience pour être prêtes à faire face aux attaques ou aux incidents majeurs", rappelle Olivier Bertin. "Elles doivent instaurer une gouvernance qui intègre la cyber-résilience et la restauration de leurs environnements. Ainsi, plutôt que d'introduire la solution d'Air Gap à travers un projet ICT standard axé sur l'infrastructure, nous l'abordons, avec nos clients, sous l'angle d'une initiative de cyber-résilience".

"Lors des échanges avec les CIOs et les responsables informatiques, il ressort en effet que ceux-ci estiment souvent qu'ils sont déjà protégés grâce aux solutions de sauvegarde qu'ils ont mises en place", confie-t-il, "par conséquent, ils ne voient pas toujours l'utilité d'ajouter une solution d'Air Gap à leur arsenal. L'adoption d'un projet d'Air Gap se fait ainsi davantage par le biais des orientations et des budgets des responsables de la stratégie de Cybersécurité ".

RANSOMWARE

UNE MENACE QUI NE FAIBLIT PAS

Les attaques de ransomware sont un véritable fléau pour les entreprises. Les conséquences peuvent être dévastatrices, allant de la perte de données critiques à l'interruption d'activité en passant par l'extorsion de sommes parfois considérables, ou encore par le paiement de frais de récupération et de remédiation conséquents portant atteinte à la réputation de l'entreprise.

Certaines idées reçues en matière de ransomware ont la vie dure. En règle générale, les légendes urbaines ont un point commun : elles peuvent conduire à développer un faux sentiment de sécurité. Dans cet article, nous vous proposerons des moyens mis à votre disposition pour protéger les solutions de dernier recours en cas d'attaque de ransomware.

5 MYTHES SUR LES RANSOMWARES

1 ***L'infection par un ransomware n'atteint pas les sauvegardes parce qu'elle s'active immédiatement***

- C'est faux. Certains ransomwares agissent comme une bombe à retardement dont l'activation est différée. Cette stratégie d'attaque a été créée précisément pour infecter les sauvegardes.

2 ***Les ransomwares n'infectent que Windows et le fait d'effectuer une sauvegarde sur un autre système d'exploitation élimine la menace***

- Les fichiers infectés peuvent être stockés sur une plateforme dans le Cloud et le cryptage y sera toujours activé.

3 ***Les ransomwares ne peuvent pas s'activer dans les sauvegardes protégées par mots de passe***

– Un fichier exécutable ne s'exécutera pas si son code a été modifié par le chiffrement. Toutefois, lorsque vous déployez cette sauvegarde pour vous rétablir d'une attaque, l'infection redevient exécutable et s'active.

4 ***Les ransomwares ne concernent que les grandes entreprises***

- Tout le monde est une cible potentielle, grand groupes, PME et mêmes citoyens. Les attaquants ont une démarche opportuniste en envoyant massivement des e-mails malveillants avec des pièces-jointes infectées sans ciblage précis. D'autres groupes d'attaquants peuvent aussi cibler des entreprises ou des individus précis. Les ordinateurs personnels des utilisateurs privés sont également régulièrement attaqués.

5 ***Il est plus facile et moins coûteux de payer la rançon plutôt que de dépenser de l'argent pour des solutions de récupération***

- Payer la rançon ne permet pas toujours d'obtenir la clé de déchiffrement. De plus, les personnes qui paient la rançon deviennent des cibles privilégiées pour une nouvelle attaque.

Le paiement ne retire pas la charge de reconstruire le système d'information et rien ne garantit l'absence d'autres codes malveillants dans les fichiers recouvrés. De surcroît, payer la rançon contribue à financer les groupes d'attaquants et en quelques sorte les financer pour lancer des attaques plus avancées sur d'autres secteurs comme l'énergie ou la santé. En effet, les ransomwares constituent un outil de financement de premier choix pour les attaquants.

DES MODES DE PROPAGATION VARIÉS

Le plus souvent les ransomwares s'introduisent dans les systèmes d'information par le biais d'emails, le code informatique malveillant déclenchant l'attaque étant directement intégré dans une pièce jointe. Les ransomwares sont souvent cachés sous une apparence anodine comme des fichiers PDF, ZIP, DOC, XLS ou même PPT. En fait, presque tous les types de fichiers peuvent être utilisés, il faut donc avoir une attention permanente. Une autre voie d'accès est celle des sites web malveillants qui affichent – non sans ironie - une notification indiquant au visiteur que son ordinateur est infecté et qu'il doit télécharger un outil pour le supprimer.

Les attaques de ransomware peuvent donc avoir des effets extrêmement néfastes pour l'organisation qui en est victime. Toutefois, les entreprises qui ont soigneusement sauvegardé leurs données peuvent se remettre d'une attaque sans avoir à payer de rançon. Pourtant, en se propageant à travers le réseau, les infections peuvent atteindre les serveurs où sont hébergées les bases de données, être transmises au système de sauvegarde et l'infecter à son tour. Assurer la sécurité des données avec des sauvegardes sécurisées est une mesure de bon sens, mais il est également nécessaire de protéger ces sauvegardes contre les ransomwares.

COMMENT PROTÉGER LES SAUVEGARDES ?

Différentes mesures peuvent réduire les risques d'infection des sauvegardes par les ransomwares, notamment :

- Séparer physiquement ou logiquement les sauvegardes de l'infrastructure principale de l'entreprise,
- Limiter les comptes et les autorisations qui ont accès aux sauvegardes,
- Utiliser des copies hors ligne sur disques durs externes ou bandes magnétiques,
- Tester régulièrement l'intégrité et la « restaurabilité " des sauvegardes,
- Segmenter le réseau en le divisant en sous-réseaux logiques et en restreignant la connectivité entre eux,
- Sensibiliser et former les employés aux bonnes pratiques en matière de cybersécurité,
- Mettre en place une solution de type Air Gap

Le concept d'Air Gap fait référence à la séparation physique ou logique entre un système informatique et tout réseau ou dispositif externe. Cette isolation garantit qu'aucune connexion ne peut être établie entre le système protégé et le reste du réseau.

En adoptant une approche d'Air Gap logique, aussi appelé Air Gap virtuel, les entreprises peuvent renforcer la sécurité de leurs sauvegardes tout en évitant certaines des limitations liées à l'Air Gap physique (soit l'isolation physique, sous sa forme la plus simple), telles que les contraintes de la gestion manuelle et les temps de récupération prolongés.

Cependant, il est important de noter que même avec une isolation logique et organisationnelle, les sauvegardes ne sont pas entièrement à l'abri des risques. Une attention constante à la sécurité, la formation du personnel sur les menaces potentielles et la mise en œuvre de meilleures pratiques de sécurité restent essentielles pour protéger efficacement les données.

GARTNER'S

BACK TO PERSPECTIVES ON CYBERSECURITY

Research firm Gartner strongly recommends that security and risk management leaders rethink their balance of investments across technology and human-centric elements when creating and implementing cybersecurity programs in line with nine top industry trends.

> *Security leaders must pivot to a human-centric focus to establish an effective cybersecurity program," according to Richard Addiscott, Senior Director Analyst at Gartner. "Focusing on people in control design and implementation, as well as through business communications and cybersecurity talent management, will help to improve business-risk decisions and cybersecurity staff retention.*

To address cybersecurity risks and sustain an effective cybersecurity program, security and risk management (SRM) leaders must be focused on 3 key domains: the essential role of ***people*** for security program success and sustainability, ***technical*** security capabilities that provide greater visibility and responsiveness across the organization's digital ecosystem, and restructuring the way the security function operates to enable ***agility*** without compromising security. Gartner says that the following 9 cybersecurity trends will have a broad impact for SRM leaders across these 3 areas.

1. HUMAN-CENTRIC SECURITY DESIGN

Human-centric security design prioritizes the role of employee experience across the control's management life cycle. "Traditional security awareness programs have failed to reduce unsecure employee behavior," says Richard Addiscott. "CISOs must review past cybersecurity incidents to identify major sources of cybersecurity induced-friction and determine where they can ease the burden for employees through more human-centric controls or retire controls that add friction without meaningfully reducing risk."

By 2027, 50% of large enterprise CISOs will have adopted human-centric security design practices to minimize cybersecurity-induced friction and maximize control adoption.

3. TRANSFORMING THE CYBERSECURITY OPERATING MODEL TO SUPPORT VALUE CREATION

Technology is moving from central IT functions to lines of business, corporate functions, fusion teams and individual employees. "Business leaders now widely accept that cybersecurity risk is a top business risk to manage – not a technology problem to solve," says Richard Addiscott. "Supporting and accelerating business outcomes is a core cybersecurity priority, yet remains a top challenge." CISOs must also connect to business value by measuring and reporting success against business outcomes and priorities.

2. ENHANCING PEOPLE MANAGEMENT FOR SECURITY PROGRAM SUSTAINABILITY

Traditionally, cybersecurity leaders have focused on improving technology and processes that support their programs, with little focus on the people that create these changes. CISOs who take a human-centric talent management approach to attract and retain talent have seen improvements in their functional and technical maturity.

By 2026, Gartner predicts that 60% of organizations will shift from external hiring to "quiet hiring" from internal talent markets to address systemic cybersecurity and recruitment challenges.

4. THREAT EXPOSURE MANAGEMENT

The attack surface of modern organizations is complex and creates fatigue. "CISOs must continually refine their threat assessment practices to keep up with their organization's evolving work practices, using a continuous threat exposure management (CTEM) approach to evaluate more than just technology vulnerabilities," recommends Richards Addiscott.

Gartner predicts that by 2026, organizations prioritizing their security investments based on a CTEM program will suffer two-thirds fewer breaches.

5. IDENTITY FABRIC IMMUNITY

Fragile identity infrastructure is caused by incomplete, misconfigured or vulnerable elements in the identity fabric. "Identity fabric immunity not only protects the existing and new IAM components in the fabric with identity threat and detection response (ITDR), but it also fortifies it by completing and properly configuring it," says Gartner's analyst.

By 2027, identity fabric immunity principles will prevent 85% of new attacks and thereby reduce the financial impact of breaches by 80%.

6. CYBERSECURITY VALIDATION

Cybersecurity validation brings together the techniques, processes and tools used to validate how potential attackers exploit an identified threat exposure. The tools required for cybersecurity validation are making significant progress to automate repeatable and predictable aspects of assessments, enabling regular benchmarks of attack techniques, security controls and processes.

Through 2026, more than 40% of organizations, including two-thirds of midsize organizations, will rely on consolidated platforms to run cybersecurity validation assessments.

7. CYBERSECURITY PLATFORM CONSOLIDATION

As organizations look to simplify operations, vendors are consolidating platforms around one or more major cybersecurity domains. For example, identity security services may be offered through a common platform that combines governance, privileged access and access management features. SRM leaders need to continuously inventory security controls to understand where overlaps exist and reduce the redundancy through consolidated platforms.

In 2022, 65% of organizations consolidated to improve risk posture while only 29% of organizations consolidated to reduce spending on licensing.

8. COMPOSABLE BUSINESSES NEED COMPOSABLE SECURITY

Organizations must transition from relying on monolithic systems to building modular capabilities in their applications to respond to the accelerating pace of business change. Composable security is an approach where cybersecurity controls are integrated into architectural patterns and then applied at a modular level in composable technology implementations. "Composable security is designed to protect composable business," Richard Addiscott underlines. This is a significant opportunity to embed privacy and security by design by creating component-based, reusable security control objects."

By 2027, more than 50% of core business applications will be built using composable architecture, requiring a new approach to securing those applications.

9. BOARDS EXPAND THEIR COMPETENCY IN CYBERSECURITY OVERSIGHT

Cybersecurity leaders must provide boards with reporting that demonstrates the impact of cybersecurity programs on the organization's goals and objectives. "SRMs leaders must encourage active board participation and engagement in cybersecurity decision making," advises Richard Addiscott. "They must act as strategic advisors, providing recommendations for actions to be taken by the board, including allocation of budgets and resources for security."

***Source**: https://www.gartner.com/en/newsroom/press-releases/04-12-2023-gartner-identifies-the-top-cybersecurity-trends-for-2023*

CLDN

RENFORCE LA GESTION DE LA SÉCURITÉ DE SON RÉSEAU

***Bart Coucke**, Head of Operations de CLDN IT Systems S.A.*

Acteur majeur de la logistique et opérateur européen de fret maritime, CLDN s'est tourné vers Telindus afin de sécuriser les échanges de données vers l'internet de ses employés - sur site, à distance - et de ses bateaux. Avec le déploiement de la solution proposée par Telindus, l'entreprise profite désormais d'un outil unique déployé depuis le cloud et intégrant un ensemble de services de sécurité. Elle a permis de flexibiliser et d'harmoniser la gestion de la sécurité sur l'ensemble du périmètre informatique du groupe.

La compagnie maritime belgo-luxembourgeoise CLDN est un opérateur majeur du fret de marchandises de part et d'autre de la Manche. Avec une flotte composée de trente navires, elle achemine des conteneurs et remorques ou encore des véhicules neufs entre les divers terminaux gérés par l'entreprise et situés à Zeebrugge (Belgique), Rotterdam et Vlissingen (Pays-Bas), Killingholme et Londres (Royaume-Uni). « Au départ de ces installations, nous proposons à nos clients un ensemble de services logistiques intégrés. Nous sommes en capacité de prendre en charge la marchandise directement auprès de l'expéditeur sur le continent, pour l'acheminer vers un de nos terminaux puis vers le destinataire final. Nous assurons le transport sur route, par bateau et le traitement des marchandises au niveau de nos terminaux », décrit Bart Coucke, Head of Operations de CLDN IT Systems S.A, la structure en charge de la gestion de l'informatique du groupe, dont l'équipe se trouve au Luxembourg.

FACILITER LA SÉCURISATION D'UN RÉSEAU ÉTENDU

La qualité d'un service logistique optimal exige de s'appuyer sur une infrastructure informatique et plus particulièrement sur un réseau solide et fiable, garantissant un échange d'information sécurisé avec l'internet.

« Il y a quelques années, nous avons été amenés à remplacer les serveurs proxys, au départ desquels nous assurions le suivi et la sécurisation des échanges avec l'internet, explique Bart Coucke. Nous nous sommes alors tournés vers Telindus, pour voir quelles solutions pouvaient répondre à nos besoins en la matière. » Telindus a alors recommandé à CLDN d'opter pour un SASE (Secure Access Service Edge). Ce concept de sécurité avait pour avantage de lui garantir la sécurité des échanges, de faciliter la gestion et le suivi des accès, d'améliorer la protection des utilisateurs et des actifs numériques de l'entreprise, qu'ils soient localisés au niveau des terminaux, des navires, du datacentre du groupe ou encore dans le cloud. *« Sur recommandation de notre partenaire, nous avons alors opté pour une solution permettant de rassembler l'ensemble des services de sécurité au niveau d'une seule instance cloud »*, commente Bart Coucke.

UNE GESTION CONSOLIDÉE ET PLUS FLEXIBLE

Grâce à cette solution, CLDN a pu consolider la gestion de la sécurité des échanges entre ses différents sites et les utilisateurs. « Lors de la crise sanitaire, alors que les solutions étaient jusqu'alors hébergées sur site ou depuis notre data center, nous avons dû recourir à des solutions cloud. Cela a impliqué d'ouvrir notre réseau. La solution mise en œuvre a facilité cette ouverture, garantissant la sécurité de la connectivité étendue au cloud public », *poursuit le responsable informatique.*

L'un des grands avantages de la solution réside dans une flexibilité accrue en matière de gestion de la sécurité. « Par le passé, il était nécessaire de déployer un ou deux pares-feux par site, et donc autant d'équipements qui demandaient un effort conséquent au niveau de la maintenance et de la supervision, poursuit Bart Coucke. L'introduction du SASE nous a permis de nous contenter d'installer des boîtiers SD-WAN, configurables à distance, facilitant grandement la gestion de ces aspects. "

CLDN, s'appuyant sur cet ensemble de solutions, gère un vaste réseau, s'étendant sur 21 sites distants.

UN ENSEMBLE DE SERVICES DE SÉCURITÉ INTÉGRÉS

La solution a, de ce fait, permis de réduire le nombre de produits nécessaires pour garantir la disponibilité du réseau et assurer la sécurité des échanges. « Elle intègre divers services de sécurité, comme des pares-feux, des outils de supervision du trafic, un Web Gateway. Toutes ces fonctionnalités peuvent être déployées et gérées à partir d'une console unique, accessible dans le cloud », précise Bart Coucke. La solution permet de déployer la même configuration de sécurité à travers l'ensemble de nos sites, à distance. " Tout est harmonisé et l'intégration d'une nouvelle entité au sein du groupe s'opère beaucoup plus facilement. « En trois jours, nous sommes parvenus à intégrer quatre nouveaux sites au réseau. Il a suffi de connecter chacun d'entre eux au moyen d'un boîtier SD-WAN. La même politique de sécurité est ainsi appliquée sur l'ensemble du réseau », précise le responsable.

SÉCURITÉ AMÉLIORÉE ET COÛTS MAÎTRISÉS

Pour Bart Coucke, le recours à une solution qui évolue sans cesse, permet à CLDN de profiter des diverses fonctionnalités, régulièrement déployées au niveau de la solution.

« En nous appuyant sur les recommandations de Telindus, partenaire historique de notre entreprise, nous sommes parvenus à améliorer la gestion de notre réseau, dans un contexte de croissance de l'activité, tout en réduisant le nombre de produits et de technologies déployées. Les mises à jour nécessaires peuvent être réalisées plus facilement, à distance, en veillant à limiter leur impact sur la production. Plus flexible, plus performante, la solution mise en œuvre répond aussi à des enjeux de maîtrise des coûts. Les frais de maintenance ont été considérablement réduits », conclut-il.

QUELLE STRATÉGIE DE CYBERSÉCURITÉ EN 2024?

La création d'une stratégie de sécurité des systèmes d'information est une étape fondamentale pour garantir la protection des ordinateurs, serveurs, réseaux, appareils mobiles, systèmes électroniques et surtout des informations de l'entreprise contre les menaces comme les attaques informatiques. Encore faut-il savoir l'adapter au métier de l'entreprise, à sa taille et à ses capacités de prise en charge.

Au-delà de la seule sécurité informatique

Une stratégie de sécurité des systèmes d'information est conçue pour maintenir un niveau de sécurité adapté aux besoins d'une organisation et reflète la vision stratégique de la direction de cette organisation. Cependant, l'objectif fondamental reste toujours le même : définir un ensemble de mesures permettant de progresser vers un niveau de sécurité à atteindre dans un délai de trois à cinq ans. Il est important de noter que la sécurité des systèmes d'information ne se limite pas à la sécurité informatique, le système d'information englobe bien plus que cela.

Au fil des années, les stratégies de cybersécurité ont évolué en réponse à l'augmentation des menaces, aux exigences des réglementations plus strictes et aux avancées technologiques. Cependant, la nécessité de développer une stratégie de cybersécurité demeure constante. Ce qui a changé depuis, c'est la méthode utilisée pour élaborer une telle feuille de route.

Au bon vieux temps des châteaux forts

Il y a 10 ou 15 ans, élaborer une stratégie de sécurité était relativement simple. On se basait alors sur des modèles conceptuels tels que le château fort pour guider la mise en place des mesures de sécurité et expliquer les choix effectués. À l'époque, les attaques semblaient plus hypothétiques, le paysage cybernétique était moins complexe, et de nombreuses entreprises partaient quasiment de zéro dans leurs efforts de cybersécurité. Ces stratégies ont principalement eu pour résultat de sensibiliser et former les directions d'entreprise, qui se sont dès lors impliquées davantage dans les discussions et les décisions.

Adapter les stratégies aux métiers

Aujourd'hui, nous ne sommes plus dans le modèle du château-fort mais plutôt dans celui de l'aéroport avec ses nombreuses interconnexions, ses multiples zones de confiance, et sa défense en profondeur, de plus en plus robuste, au fil des contrôles de sécurité du fait du zero-trust. Dès lors une simple discussion ne suffit plus, car certaines grandes entreprises investissent des sommes considérables dans la cybersécurité. Les mesures de sécurité de base, telles que les mises à jour et la protection périphérique, sont désormais complétées par un éventail de dispositions de plus en plus spécifiques, remettant en question l'idée d'un schéma unique.

Une approche différenciée par entité

Ainsi, une approche pragmatique et flexible, alignée sur les priorités commerciales et industrielles, est essentielle. Les premières étapes consistent à définir la méthodologie qui apportera de la rigueur et de la crédibilité, à la fois vis-à-vis de la direction et des régulateurs. Concrètement, il s'agit d'établir un cadre – le "framework" - de cybersécurité de l'organisation et - pour les grandes structures - une méthode permettant à chaque entité de définir ses propres objectifs au sein de ce cadre. La stratégie unique cède la place à une approche différenciée par entité.

Choisir un cadre de référence

Au Luxembourg, l'approche ISO 27001 est largement reconnue et repose sur un système de management visant à améliorer – de façon continue - la mise en œuvre de la sécurité basée sur les risques.

D'autres Frameworks existent, il est essentiel d'adopter celui qui est aligné avec la culture de l'entreprise et de l'écosystème dans lequel elle évolue. Il est également important que le Framework soit basé sur une référence du marché telle que ISO, NIST ou bien BSI. La plupart des entreprises personnalisent les contrôles en les adaptant à leurs besoins spécifiques. Le cadre choisi est également utile pour fournir une bibliothèque de mesures de sécurité sur laquelle l'entreprise pourra s'appuyer pour opérationnaliser sa stratégie avec la traçabilité dans le cadre choisi.

Avec le cadre établi, il est important de décliner la stratégie par activités via la formulation d'objectifs spécifiques pour chacune. Dans le cas d'une grande entreprise, une cible commune est souvent imposée par le groupe pour assurer le respect par les filiales des fondamentaux de sécurité. Chaque entité doit ensuite définir sa propre cible en fonction de ses besoins spécifiques, ce qui peut s'avérer complexe en termes de correspondance entre les contrôles du cadre et les risques identifiés. Quelle que soit la taille de l'entreprise, la collaboration étroite avec les équipes de gestion des risques est souvent nécessaire pour parvenir à un équilibre.

Managed Services

La plupart des dirigeants ont compris qu'il devenait urgent de hausser le niveau de sécurité de leur organisation. Les entreprises se sont notamment équipées de solutions d'EDR - solutions de protection des terminaux utilisant des analyses en temps réel et une automatisation basée sur l'IA - pour contrer la menace des ransomware, mais beaucoup n'ont ni les moyens ni la volonté de former des équipes de sécurité capable de traiter les alertes remontées par ces outils 24 heures sur 24 et 7 jours sur 7.

Les CIO se sont mis à la recherche de partenaires afin de réaliser ces tâche astreignantes et très coûteuses. Le modèle "managé" y apporte une réponse et les éditeurs de solutions de sécurité ne s'y sont pas trompés : ces dernières années, ils ont largement développé leurs réseaux de MSSP (Managed Security Service Providers) pour diffuser leurs produits, notamment auprès du midmarket et des PME. Le marché mondial des services de cybersécurité managés devrait ainsi passer de 15,7 milliards de dollars en 2023 à 32,68 milliards de dollars d'ici 2030 [1].

[1] *https://www.fortunebusinessinsights.com/cyber-security-managed-services-market-106883*

Cloud et partenaire : la combinaison gagnante ?

De plus en plus de "briques de sécurité" sont proposées "as-a-service" par leurs éditeurs et sont assorties d'offres managées assurées par des partenaires. C'est le cas des EDR et des SIEM et également des SOC (Security Operations Center), mais aussi d'autres "briques" telles que les solutions de gestion d'identité et des accès aux applications (IAM), de Firewall as a Service, de WAF (Web Application Firewall) ou encore de protection des endpoints (EPP) qui ne peuvent se passer du Cloud pour le sandboxing ou faire tourner leurs algorithmes d'IA les plus avancés. Dans certains domaines, comme la Threat Intelligence, la mutualisation du service entre de multiples clients est même une composante clé du business model. En conséquence, le marché de la cybersécurité « as a service " devrait atteindre 46,6 milliards de dollars d'ici 2030, avec un taux de croissance annuel moyen de 17,5 % sur la période 2023-2030 [2].

[2] *https://www.meticulousresearch.com/product/cybersecurity-as-a-service-market-5506*

LA ROADMAP CYBER SÉCURITÉ DE TELINDUS

Les six piliers de la cybersécurité tels que conçus par Telindus sont indispensables pour sécuriser votre transformation digitale et vous faire bénéficier d'une approche 360° de la cybersécurité. Ces quelques pages vont vous permettre de comprendre et appréhender les services proposés et leur utilité au sein de votre organisation.

PREVENTIVE
Se préparer à l'imprévisible en gérant les risques d'entreprise.

DEFENSIVE
Protéger vos ressources les plus sensibles contre les menaces et les attaques.

DETECTIVE
Surveiller et détecter promptement les vulnérabilités, les menaces et les tentatives d'attaques.

REACTIVE
Réagir après un incident pour reprendre vos activités le plus rapidement possible en minimisant les impacts sur vos opérations et vos clients.

OFFENSIVE
Identifier vos faiblesses avant qu'elles ne soient exploitées contre vous par des attaquants.

PROACTIVE
Anticiper les mouvements des attaquants pour y répondre avant même qu'ils ne frappent.

*Cédric Mauny, **Strategic Advisor Cybersecurity** nous explique la genèse du portfolio sécurité et cybersécurité de l'entreprise: « Telindus est présent sur le marché ICT depuis près de 45 ans et a surfé, traversé et même parfois influencé les plus grandes évolutions du domaine au Luxembourg. L'aspect technique fait partie de notre ADN et c'est sur cette base que nous avons construit et façonné un ensemble de compétences pour soutenir nos clients à chaque étape de leur évolution mais également de celle du marché. »*

« Compte tenu de l'accélération de ces dernières années, il était évident pour nous d'aller vers une structuration de nos activités de sécurité et cybersécurité en grands piliers. Le but étant d'offrir aux clients la garantie d'un conseil et d'un support modulaire, permettant d'adresser leurs propres spécificités. Lorsque nous mettons en place des solutions taillées sur mesure pour nos clients, nous proposons une approche globale et intégrée présentée sous la forme d'un modèle de sécurité complet dans laquelle le client arrive à un moment précis, à une étape définie selon son profil de risque et son niveau de maturité où Telindus l'accompagne conformément à sa vision « secure the digital journey of our customers ».

PREVENTIVE

L'un des piliers sur lesquels repose l'offre de services de cybersécurité de Telindus est d'ordre préventif et a pour objectif de préparer les organisations à faire face aux défis de sécurité avant même qu'un incident ou une situation tendue ne se produise.

"Pour cela, nous mettons en place chez nos clients un environnement organisé, structuré et compétent pour aborder les problématiques de cybersécurité", explique Frédéric Hauss, Responsable Technique Cybersecurity Services chez Telindus. "Cela comprend plusieurs éléments, tels que la formation et la sensibilisation du personnel aux questions de sécurité, notamment la gestion des mots de passe, la sensibilisation au phishing et les bonnes pratiques à adopter lors de la réception de courriels".

Parallèlement, vous pouvez avoir recours à des services d'accompagnement organisationnel et de conformité tels que "CISO as a Service", proposé aux entreprises qui n'ont pas les ressources nécessaires ou le besoin de disposer - en permanence - d'un responsable de la sécurité des systèmes d'information. Ces services sont ponctuels et adaptés aux besoins spécifiques des clients.

L'analyse de risques, quant a elle, est une autre facette importante de ce volet préventif. Elle permet d'étudier l'environnement de chaque client, d'identifier les sources de risques potentielles et de les évaluer. Cette démarche vise également à accroître la prise de conscience au sein de l'entreprise et à élaborer des plans d'action pour atténuer ces risques en fonction de leur priorité.

"Nos activités de "policies analysis" – c'est-à-dire d'analyse des règles en place - et de consultance consistent à déléguer des experts auprès de nos clients pour évaluer la configuration de leurs infrastructures", ajoute Fréderic Hauss. L'objectif est ici de vérifier si les meilleures pratiques en matière de sécurité sont respectées et si des améliorations peuvent être apportées à ce niveau. Il s'agit d'une approche centrée sur l'humain, l'organisation et l'analyse des processus en place, qui n'aborde pas les aspects liés aux projets d'infrastructure ou de déploiement".

En résumé, cette gamme de solutions vise à anticiper les incidents potentiels en proposant aux entreprises les meilleures conditions préalables pour faire face à toute situation de manière optimale, avant même que ces incidents ne se produisent.

DEFENSIVE

L'un des premiers remparts contre les cyberattaques est la mise en place et la gestion des infrastructures de défense. Pour se protéger des attaques internes et externes, il est primordial de gérer les solutions de sécurité de façon quotidienne. Seule une gestion sans faille est synonyme de sécurité. Le périmètre à couvrir est très large et demande une attention quotidienne avec un haut niveau d'expertise pour les infrastructures plus complexes.

Ce volet défensif d'une stratégie de cybersécurité permet de fournir une protection aux infrastructures en mettant en place divers services de défense. Il agit en tant que barrières frontales

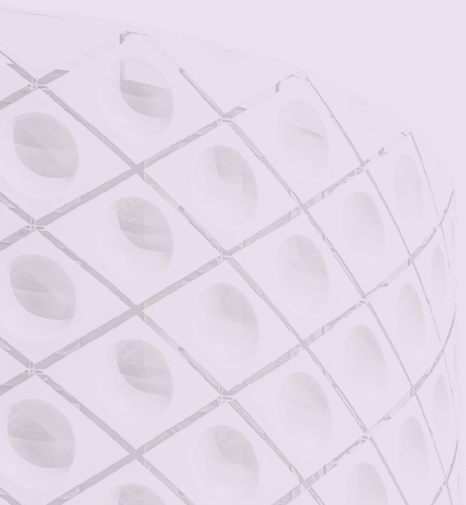
pour les ressources accessibles par les utilisateurs internes et externes, par exemple pare-feu, web et mail security gateways, web application firewall explique Yvon Boutry, Tribe leader security. On y retrouve également les nouveaux services DNS securité qui, en mode défensif, se concentrent sur la protection des protocoles inévitablement utilisés pour entrer et sortir de l'infrastructure.

On distingue trois catégories d'environnements : les clients avec leur propre infrastructure (on premises datacenter), ceux qui utilisent les services de cloud public comme Azure, AWS ou Google, et enfin les services d'hébergement privé (hosted private cloud), tels que le U-Flex de Telindus. Souvent, les clients opèrent dans plusieurs de ces environnements en même temps, donnant lieu à des environnements de type hybrides.

Chacun de ces environnements a ses spécificités en terme de sécurité défensive, mais ces systèmes de défenses doivent être cohérents, homogènes et impérativement communiquer entre eux. Dans un environnement hybride, une faille à une extrémité permettra potentiellement à l'assaillant de se propager sur l'ensemble des systèmes précise Laurent Untereiner, Head of Sales Unit – Network & Security.

Telindus peut supporter ces activités sur plusieurs axes :

- Intégration et déploiement
- Gestion des incidents et investigation
- Veille des vulnérabilités et gestion des patchs
- Gestion de la supervision
- Gestion des requêtes
- Suivi technique et conseil sur la stratégie de l'infrastructure sécurité
- Rapport d'activité sécurité



DETECTIVE

Le service CSIOC (Cyber Security & Intelligence Operations Center) de Telindus propose des services de surveillance avancée pour anticiper, détecter et réagir le plus rapidement possible en cas d'attaque. En s'appuyant sur les technologies de pointe en matière de Threat Intelligence, de Machine Learning et d'automatisation, ce service CSIOC apporte des capacités de détection adaptées pour permettre une réaction rapide sur des anomalies détectées dans votre Système d'Information. La surveillance accrue et l'analyse des ingénieurs de Telindus en cas d'alerte réduisent considérablement le temps moyen de résolution des incidents et permettent aux clients de se concentrer sur leurs activités.

Pour illustrer, ce service est souvent comparé à une tour de contrôle surveillant l'ensemble de l'infrastructure, c'est-à-dire le système d'information et tous ses composants matériels.

"Il s'agit ici de repérer tout comportement inhabituel pouvant indiquer une activité malveillante, une intrusion ou toute autre menace potentielle", explique Frédéric Hauss, "Plus l'entreprise dispose d'équipements/solutions défensifs doublé d'une architecture sécurisée, plus notre visibilité sur le trafic réseau et comportement inhabituel augmente".

Le Log Management, qui est l'un des services de la fonction détection, consiste à collecter, normaliser, enrichir (catégorisation…), analyser et 'archiver les journaux d'activité de l'ensemble du système d'information. Ces journaux enregistrent des événements de type Sécurité (authentification, création/suppression utilisateur, clé de registre…), Système (lancement/arrêt des services, debug…), Applicative et Transactionnel, et permettent ainsi pour le service Security Monitoring & Alerting de détecter en temps réel des comportements potentiellement malveillants.

La détection « comportement inhabituel » est basée sur un ou plusieurs évènements corrélés entre eux selon des critères basés sur les Tactiques, Techniques et Procédures (TTPs) décrites dans la matrice Mitre ATT&CK.

Le service de Security Monitoring & Alerting, quant à lui, génère des alertes vers les équipes de sécurité lorsqu'un événement suspect est détecté. Le traitement des alertes est alors automatisé grâce au service SOAR - Security Orchestration, Automation & Response, qui regroupe un ensemble de technologies permettant de réagir (semi-) automatiquement à certains incidents

En effet, un SOC a pour vocation de recevoir une multitude d'informations (logs/alertes) qui sont traitées pour cibler uniquement les évènements importants à investiguer. Suivant l'analyse des ingénieurs des recommandations sont fournies dans le contexte d'un niveau de service défini afin de mitiger ou éradiquer une attaque.

REACTIVE

Lorsqu'une alerte est signalée aux équipes SOC (Security Operation Center), il se peut que certaines informations ne puissent être analysées en raison de leur caractère incomplet ou inexistant. C'est à ce moment-là indique Fréderic Hauss que la force réactive entre en jeu, soit pour mener une enquête de type "forensic" - similaire à une investigation médico-légale, sur la ressource concernée par l'alerte - soit pour procéder à une recherche proactive de menaces, appelée "Threat Hunting", afin de déterminer l'étendue de l'incident en recherchant, dans l'ensemble du réseau, des indicateurs de compromission (IoC) correspondant à des modèles ou des schémas d'attaques.

Ces schémas d'attaques peuvent être connus et répertoriés par la communauté mondiale de la cyberdéfense, mais il est également possible que l'enquête « forensic " révèle de nouveaux schémas inconnus jusqu'alors. Les attaques de type 0 day ont la particularité de passer outre les équipements de défense mis en place par les entités. Les investigations type forensics ont la particularité d'analyser en post mortem les activités de l'attaquant pour découvrir le patient 0 et les tactiques, techniques et procédures (TTP) employés par l'attaquant pour compromettre le système d'information d'une entité explique Fréderic Hauss.

Dans le cadre de cette approche réactive, la gestion de crise - Crisis Management -, consiste à mettre en place une force d'intervention ayant pour mission de comprendre la nature de l'incident, de le contenir et de proposer un plan de remédiation. Cette task force est parfois composée de membres de différentes équipes au sein de Telindus.

Telindus au travers de sa multitude d'activités est à même de fournir des services de remise en place de l'activité d'une société après un incident ayant provoqué une interruption des services du clients. Que ce soit sur site, au travers de nos datacentres privés ou des services de cloud public, Telindus est en capacité de remonter un système d'information pour un client à l'arrêt. La production du client est restaurée et sont niveau de sécurité est améliorée pour éviter que l'incident de sécurité à l'origine de la perturbation ne se reproduise. Cette task force a déjà prouvé son efficacité pour plusieurs clients et est un avantage conséquent sur la place luxembourgeoise.

OFFENSIVE

Le volet offensif d'une stratégie de cybersécurité implique de tester et de mettre à l'épreuve les infrastructures d'un système d'information en utilisant les mêmes techniques que celles employées par les attaquants. Le principal objectif est de découvrir, lors de l'évaluation du réseau, des vulnérabilités exploitables par des individus malveillants, selon des schémas d'attaque bien définis.

"Pour identifier de telles vulnérabilités", nous dit Frédéric Hauss, "nos équipes effectuent des tests basés sur deux méthodologies d'évaluation différentes, à savoir OSSTMM (Open Source Security Testing Methodology Manual) et OWASP (Open Web Application Security Project), qui prennent la forme de tests d'intrusion et d'actions d'ingénierie sociale. Nous recourons également à des tests d'intrusion physique, où une équipe spécialisée tente de pénétrer dans les locaux du client ayant souscrit ce type de service pour récupérer des informations utiles, en copiant par exemple des badges d'accès, en soudoyant des membres du personnel ou en exploitant simplement certaines faiblesses humaines".

La simulation d'attaque vise, quant à elle, à évaluer l'efficacité des mesures mises en place par une entreprise pour faire face à une cyberattaque. Dans ce cas, les spécialistes de Telindus utilisent des méthodes utilisées par des cybercriminels dont les profils sont connus et répertoriés dans des référentiels tels que MITRE ATT&CK, une base de connaissances mondiale répertoriant et décrivant les cyberattaques et les intrusions

"Nous pratiquons également des exercices de Red Team", ajoute Olivier Trientz, Business Developer Security & Cyber-Security chez Telindus. "Le Red Teaming est une activité basée sur des objectifs qui nécessitent une vision globale de l'organisation du point de vue de l'attaquant. L'objectif d'une campagne de type Red Team est de démontrer comment les attaquants, dans le monde réel, peuvent combiner des actions apparemment sans rapport pour atteindre leurs objectifs". Contrairement aux tests d'intrusion, ce type de campagne ne se limite pas à un périmètre restreint au sein des infrastructures de l'entreprise et peut s'inscrire sur le long terme.. L'extension logique consiste en la réalisation des exercices Threat Intelligence-based Ethical Red Teaming (TIBER-EU et sa déclinaison luxembourgeoise gérée par la CSSF) qui sont basés sur un cadre européen de cyberattaque contrôlée visant à tester la résilience des entités critiques dans un contexte de risque systémique de l'écosystème financier. L'objectif de ces exercices grandeur nature est de mettre sous pression les points faibles des mécanismes de défense pour mieux les renforcer.

PROACTIVE

Le dilemme entre « prévenir ou guérir » existe également dans le domaine de la cybersécurité. Une approche proactive comprend l'identification préventive des faiblesses en termes de sécurité et la mise en place de processus pour identifier les menaces avant qu'elles ne surviennent. La cybersécurité proactive englobe toutes les mesures défensives nécessaires pour protéger le système d'information d'une organisation contre les cyberattaques.

"De plus en plus, les équipements de sécurité sont conçus pour recueillir des informations dans le Cloud, telles que les métadonnées ou les signatures, afin de détecter des signes d'attaques beaucoup plus complexes", indique Fréderic Hauss. " Face aux menaces actuelles - comme les attaques avancées ou les vulnérabilités zero-day - la mise en corrélation de signaux faibles ainsi que leur analyse par des services cloud, nous permettent d'identifier des dangers potentiels. Ces informations enrichissent notre base de connaissances, que nous partageons ensuite avec des référentiels mondiaux. Les solutions cloud modernes associent des fonctions avancées de Machine Learning et différentes sources de Threat Intelligence pour identifier efficacement différentes tactiques et techniques répertoriées dans les principaux référentiels mondiaux tels que MITRE ATT&CK, tout en réduisant les faux positifs. Cela permet aux équipes de sécurité de se concentrer sur l'investigation et la remédiation des incidents les plus graves, sans être submergées par un trop grand nombre d'alertes".

Les techniques d'Adversary Emulation et d'Adversary Simulation, qui relèvent également de ce volet proactif, sont utilisées pour évaluer la protection en place. Bien que ces termes soient souvent utilisés de manière interchangeable, ils présentent des différences notables.

L'Adversary Emulation est une approche ciblée qui consiste à reproduire de manière identique les tactiques, techniques et procédures (TTP) employées par un acteur malveillant connu. Son objectif principal est d'imiter au mieux le comportement de cet adversaire identifié, permettant ainsi à l'organisation d'évaluer et de renforcer ses mécanismes de défense contre cette menace connue. Pour ce faire, une compréhension approfondie du modus operandi de l'adversaire est nécessaire, acquise grâce à la Threat Intelligence, afin de fournir une perspective précise et spécifique aux vulnérabilités de l'organisation.

L'Adversary Simulation est un processus plus étendu qui implique de simuler les comportements potentiels d'un adversaire au cours d'une attaque contre les systèmes d'une organisation. Contrairement à l'Adversary Emulation, elle ne se limite pas strictement aux TTP d'un acteur spécifique. L'Adversary Simulation offre la liberté d'incorporer une variété de tactiques et de techniques, allant au-delà de celles utilisées par les adversaires connus. C'est une approche plus souple et polyvalente, destinée à mettre en évidence un éventail plus large de vulnérabilités potentielles.

ZOOM SUR...
MANAGED SECURITY SERVICES

Au sein de Telindus, l'activité d'infogérance de la sécurité informatique, communément appelée Managed Security Services (MSS), est relativement récente. "Historiquement, nous avons débuté en gérant et en opérant les infrastructures et les réseaux de nos clients", rappelle Yvon Boutry. "Avec le temps, nous avons constaté que la sécurité prenait une place de plus en plus prépondérante, devenant la principale préoccupation de nos clients".

La cybersécurité requiert cependant des solutions délicates et complexes, et il arrive souvent que le client n'ait pas les capacités internes nécessaires pour gérer ce type de solutions. Alors que le cycle de renouvellement des produits de sécurité est d'environ trois ans, il peut s'étendre jusqu'à six ans pour les produits réseau, par exemple. Pour les entreprises qui doivent gérer elles-mêmes leurs infrastructures et acquérir les différents composants de leur système de sécurité, cela implique de disposer de personnel formé et toujours disponible, ainsi que d'assimiler de nouvelles technologies, en plus des tâches quotidiennes de leurs équipes. Par conséquent, il devient de plus en plus difficile pour une entreprise de faire face à la complexité et au rythme de renouvellement des solutions de sécurité.

"C'est là que recourir aux Managed Security Services prend tout son sens", souligne Laurent Untereiner. "En externalisant tout ou partie de la responsabilité de la sécurité de son système d'information à un prestataire de services comme Telindus, une entreprise bénéficie de compétences, d'une connaissance des équipements, d'un suivi et d'une réactivité en cas de panne ou d'incident qu'elle ne peut pas assurer seule sans consentir à des investissements considérables. Notre rôle est d'accompagner notre client, d'effectuer le suivi et la prise en charge complète ou partielle de ses besoins en matière de cybersécurité. Nous agissons également de manière proactive pour maintenir et faire évoluer son infrastructure en adéquation avec les meilleures pratiques".

La disponibilité des infrastructures prend aujourd'hui une importance grandissante. Lorsqu'un client opte pour ce modèle de service, il ne demande plus au prestataire d'effectuer des tâches spécifiques, mais d'assurer un service de sécurité avec des temps d'indisponibilité tolérables prédéterminés, garantis par différents niveaux de SLA (Service Level Agreements).

"De plus en plus d'entreprises souhaitent passer à ce mode en raison de la complexité croissante dans le domaine de la sécurité et de la difficulté de maintenir des équipes en nombre suffisant", constate Olivier Trientz.

Telindus dispose des ressources nécessaires pour assurer ces services, notamment la prise en charge des aspects opérationnels 24 heures sur 24 et 7 jours sur 7, la réalisation des mises à jour, l'évaluation des besoins et le déploiement des moyens nécessaires pour sécuriser les infrastructures, ainsi que le maintien d'une veille que le client n'a souvent pas les moyens financiers et humains d'effectuer.

ZOOM SUR...
LE CSIOC, TOUR DE CONTRÔLE INTELLIGENTE

Un centre opérationnel de sécurité (Security Operations Center ou SOC) est une plateforme centralisée animée par une équipe de sécurité dont la fonction est de superviser, détecter, analyser et prendre en charge les incidents de cybersécurité, 24 heures sur 24 et 7 jours sur 7.

Dans le cas de Telindus, il convient plutôt de parler de CSIOC ou Cyber Security & Intelligence Operations Center. Il s'agit en réalité d'un SOC amélioré dont l'objectif principal est d'analyser les violations de sécurité et les incidents historiques afin d'identifier des modèles. Le CSIOC utilise ces informations, recueillies au fil du temps, pour identifier les anomalies et prévoir les violations avant qu'elles ne se produisent. Les renseignements internes, associés aux informations de threat intelligence provenant de sources externes, sont réinjectés dans le système pour permettre l'automatisation de certaines réponses prédéfinies à des violations probables.

Le CSIOC ne doit pas seulement identifier les menaces, il doit aussi les analyser, explorer la source, produire des rapports sur les vulnérabilités découvertes et mettre des mesures en place pour empêcher des problèmes similaires de se produire. En d'autres termes, il traite les problèmes de sécurité en temps réel tout en cherchant continuellement des moyens d'améliorer la position de sécurité de l'entreprise.

"Le CSIOC de Telindus adopte une approche en cascade de la gestion des problèmes de sécurité, dans laquelle les analystes et les ingénieurs sont catégorisés en fonction de leurs compétences et de leur expérience. Ce sont des professionnels spécialement formés pour superviser et gérer les menaces de sécurité. Non seulement ils sont qualifiés dans un large éventail d'outils de sécurité, mais ils connaissent les processus spécifiques à suivre en cas d'incident", explique Olivier Trientz.

NIVEAU 1

La première ligne de réponse aux incidents est le Niveau 1. Cette équipe guette les alertes et déterminent leur urgence pour les transmettre, éventuellement, au Niveau 2. Le personnel du Niveau 1 peut également gérer des outils de sécurité et produire des rapports réguliers.

NIVEAU 2

Les spécialistes du Niveau 2 possèdent plus d'expertise, ce qui leur permet d'aller rapidement à la racine du problème et d'évaluer quelle partie de l'infrastructure est attaquée. Ils suivent des procédures pour corriger les défaillances et rétablir les systèmes, et signalent les problèmes méritant une investigation supplémentaire.

NIVEAU 3

Le Niveau 3, fait intervenir des analystes de sécurité de haut niveau qui recherchent activement les vulnérabilités du réseau. Ils emploient des outils de détection des menaces avancées pour diagnostiquer les faiblesses et produire des recommandations afin d'améliorer la sécurité globale de l'entreprise. Ce groupe compte également parmi ses membres des spécialistes tels que des enquêteurs de type forensic et des contrôleurs de conformité.

"Pour résumer, un CSIOC n'est pas uniquement un ensemble d'outils. Il faut plutôt le considérer comme a un écosystème où interagissent des personnes, des solutions et des techniques", nuance Frédéric Hauss. En utilisant une combinaison complexe d'outils et de talents choisis pour superviser et gérer l'intégralité du réseau, le CSIOC remplit plusieurs fonctions, de la supervision proactive et permanente des réseaux, des machines et des logiciels à l'analyse, l'investigation et la documentation des tendances en cybersécurité sécurité, en passant par l'application des politiques et procédures de sécurité, la recherche et la prise en charge des virus, malwares et ransomwares à l'aide de solutions adaptées ou encore la recherche des causes profondes des attaques afin de prévenir de futurs problèmes.

"Naturellement, ajoute Olivier Trientz, "tous ces services font l'objet de rapports périodiques et de réunions de suivi avec les clients, ce qui permet de proposer et de mettre en place des mesures correctives et d'évaluer l'efficacité des interventions du CSIOC. Une bonne gouvernance et un partenariat fort avec nos clients sont les éléments du succès".

Le CSIOC de Telindus est certifié ISO 27001 et sa mise en œuvre est réalisée en suivant les exigences du référentiel PDIS (Prestataires de détection d'incidents de sécurité) de l'ANSSI française, apte à assurer une supervision de la sécurité des infrastructures critiques.

CONCLUSION

Pour conclure, la cybersécurité est nécessaire mais pas suffisante : « Notre force repose sur les compétences de nos collaborateurs pour apporter à nos clients le meilleur de l'expérience acquise au fil des années et s'appuie également sur l l'ensemble des autres équipes de Telindus pour bénéficier de toutes les capacités ICT : cloud, systèmes, storage, télécom, ... » explique Cédric Mauny.

« Actuellement, il ne se passe pas un jour sans qu'un incident de sécurité soit la cause de l'arrêt d'une entreprise.Dans un tel contexte, ce qui compte c'est la capacité d'un redémarrage rapide en total sécurité de l'activité métier, cela nécessite des compétences pluridisciplinaires qui vont au-delà de la seule cyber-sécurité dans le but de reconstruire des infrastructures ICT sous la guidance des équipes de gestion de crise cyber. Les clients peuvent entièrement faire confiance à Telindus pour ceci. » conclut l'expert.

YVES LE TRAON

LA SYNERGIE ENTRE L'ÉDUCATION, LA RECHERCHE ET L'INDUSTRIE EST UNE COMBINAISON DÉTERMINANTE POUR LE LUXEMBOURG

AVEC CÉDRIC MAUNY

***Yves Le Traon**, Vice-Directeur du SnT Centre*

*Le 1er janvier 2024, le professeur **Yves Le Traon** succédera à Björn Ottersten au poste de directeur du SnT. A quelques mois de sa prise de fonction, nous avons pris un peu de temps pour échanger avec lui sur quelques sujets d'actualité et esquisser, - avec **Cédric Mauny**, Strategic Advisor Cybersecurity chez Telindus - les évolutions et priorités pour l'industrie de la cybersécurité, pour les entreprises et pour le centre de recherche technologique de L'Université du Luxembourg.*

L'IA, AVEC CHATGPT ET MIDJOURNEY NOTAMMENT, A INDISCUTABLEMENT FAIT LE BUZZ CETTE ANNÉE. SOMMES-NOUS RÉELLEMENT À L'AUBE D'UNE "RÉVOLUTION IA" OU ASSISTONS-NOUS PLUS SIMPLEMENT AUX PREMIERS PAS D'UNE INTELLIGENCE ARTIFICIELLE MISE À LA PORTÉE DU PLUS GRAND NOMBRE ?

• **Y.L.T.** Avec ChatGPT, l'intelligence artificielle a fait une entrée soudaine dans nos vies quotidiennes. Le premier effet que cela a eu sur moi, c'est l'émerveillement. Il s'agit tout de même d'une avancée incroyable ! Il semble que ce type d'agent conversationnel passe le test de Turing haut la main : c'est une avancée historique. Bien sûr, après l'émerveillement, viennent les questions: Quels sont les risques associés ? Quelles sont les limites réelles ? Mais il est indéniable que cela ressemble à une révolution. Avec ChatGPT, l'IA a démontré sa capacité à générer ou modifier du contenu sémantiquement riche d'une manière comparable à celle des êtres humains, voire même de manière plus efficace en termes de temps.

• **C.M.** À mon sens, la grande révolution apportée par ChatGPT réside dans sa facilité d'accès à l'IA. La vraie innovation apportée par OpenAI, c'est cette interface incroyablement conviviale, mise à disposition de tout un chacun.

Il faut cependant rappeler qu'une IA n'est guère capable de remettre en question une réponse : contrairement à un être humain, elle ne doute pas. C'est pourquoi nous ne pouvons pas nous fier à 100% aux modules d'IA intégrés aux outils informatiques actuels. Seuls les êtres humains possèdent encore cette capacité unique à replacer une réponse dans un contexte plus large et à opérer une réflexion sur leurs propres actions. C'est pourquoi il est indispensable d'informer les utilisateurs sur les limites de ce que ces systèmes peuvent produire. Il faut également souligner que l'on ne peut pas simplement utiliser tel quel ce qu'une IA a généré, sous peine de s'exposer à de dangereuses conséquences.

L'USAGE GÉNÉRALISÉ DE L'IA DANS DIFFÉRENTS SECTEURS NE MANQUE PAS DE SOULEVER DES QUESTIONS ÉTHIQUES : ANOMALIES DANS LES DONNÉES D'ENTRAÎNEMENT, MISE EN DANGER DE LA CONFIDENTIALITÉ DES INFORMATIONS PERSONNELLES SENSIBLES OU ENCORE RESPONSABILITÉ EN CAS DE PRÉJUDICE RÉSULTANT DE L'UTILISATION DE CES SYSTÈMES. COMMENT GARANTIR QUE CES TECHNOLOGIES SOIENT UTILISÉES DE MANIÈRE RESPONSABLE ET ÉTHIQUE ?

• **Y.L.T.** En fin de compte, ce que nous souhaitons tous c'est que l'être humain conserve le contrôle sur l'IA et je pense que cela s'inscrit également dans la lignée de l'Artificial Intelligence Act et des réflexions menées au niveau européen. Il ne faut pas la craindre, mais plutôt l'apprivoiser et comprendre ses limites. Par conséquent, il est nécessaire d'accorder à l'éducation et à la formation toute l'importance qu'elles méritent. Les utilisateurs doivent prendre conscience de ce qui est réalisable avec une IA tout en reconnaissant leur propre responsabilité à cet égard.

• **C.M.** Dans le même ordre, ce qui me préoccupe est l'homogénéisation de la pensée induite par une utilisation généralisée de ChatGPT. Mon inquiétude réside dans le fait que tout le monde recourt constamment à cet outil, nous finirons par obtenir des résultats uniformes, un nivellement vers une qualité médiane et consensuelle en quelque sorte.

• **Y.L.T.** Je suis convaincu qu'il existe en effet de tels risques. Tout d'abord, il y a le risque bien connu aujourd'hui de propagation des biais qui sont inhérents aux données d'entraînement. Bien que des efforts soient déployés pour atténuer ces problèmes, il demeure extrêmement difficile de les éviter entièrement. Ensuite, il y a le danger que nous renoncions à notre propre intelligence, en quelque sorte. Nous devons conserver le contrôle et la maîtrise sur l'IA. La tentation de ne plus penser par nous-mêmes, de ne plus créer de contenu de manière autonome, en raison de l'efficacité et de la rapidité apportées par l'IA est une tendance à laquelle il est essentiel de prendre garde. Cela peut conduire à un risque de nivellement, peut-être pas un nivellement vers le bas, mais vers une certaine qualité médiane.

C.M. Effectivement, il est essentiel que les utilisateurs soient bien informés des limites actuelles de ces outils. Il faut se rappeler, par exemple, que ChatGPT n'a aujourd'hui pas accès à Internet et ne possède à ce jour aucune connaissance au-delà de l'année 2021. Qui est conscient de ces limites ? Cette problématique relève essentiellement de l'apprentissage de l'outil. De plus, ChatGPT doit être utilisé dans des contextes appropriés, avec des règles bien connues de celui qui l'utilise, et également dans le cadre d'applications bien spécifiques, comme la manipulation de texte, où les résultats obtenus sont remarquables.

• Y.L.T. Je partage totalement l'avis de Cédric. Les IA que nous développons actuellement pour l'industrie sont très spécifiques et répondent à des besoins précis. Pour utiliser ces technologies de manière appropriée, une compréhension approfondie du contexte et des exigences est indispensable.

L'UNI A RÉCEMMENT LANCÉ, AVEC D'AUTRES UNIVERSITÉS EUROPÉENNES, UN MASTER EN CYBERSÉCURITÉ DÉNOMMÉ CYBERUS AFIN DE FORMER UNE NOUVELLE GÉNÉRATION D'EXPERTS EN CYBERSÉCURITÉ. POUR LEUR PART, LES ENTREPRISES METTENT EN PLACE DES PROGRAMMES D'UPSKILLING ET DE RESKILLING POUR RÉDUIRE LA PÉNURIE DE COMPÉTENCES QUI AFFECTE LE SECTEUR. COMMENT L'ÉDUCATION, LA RECHERCHE ET L'INDUSTRIE PEUVENT-ELLES AVANCER ENSEMBLE POUR REMÉDIER À CETTE CARENCE ?

• Y.L.T En matière de cybersécurité, il est indispensable de bien comprendre les besoins de l'écosystème pour y répondre de manière adéquate. En ce sens, la synergie entre l'éducation, la recherche et l'industrie est une combinaison déterminante pour le Luxembourg.

En ce qui concerne l'enseignement, l'Université du Luxembourg collabore depuis plus de quinze ans avec le LIST pour proposer un Master en Management de la Sécurité des Systèmes d'Information. Elle vient par ailleurs de lancer un programme de Master Erasmus Mundus en cybersécurité baptisé CYBERUS, en collaboration avec l'Université de Bretagne Sud et l'Université Libre de Bruxelles.

Pour ma part, je considère qu'il serait souhaitable de développer un master complet au Luxembourg, avec une composante significative en intelligence artificielle, voire un parcours intégral en cybersécurité, de la formation initiale jusqu'au master.

Enfin, il ne faut pas négliger le volet de la formation doctorale où le SnT forme actuellement près de 200 doctorants. Nous disposons déjà de ce vivier de talents, mais nous nous devons le développer davantage.

• C.M. CYBERUS est un projet extrêmement intéressant. Le CLUSIL, l'association des professionnels de la cybersécurité du Luxembourg, y apporte d'ailleurs son soutien et travaille à en accroître la visibilité au sein de la communauté cyber et auprès des entreprises. Par ailleurs, en tant qu'acteur majeur dans le domaine de l'ICT, Telindus soutient activement la nouvelle législation luxembourgeoise concernant les métiers en situation de pénurie, parmi lesquels on retrouve la cybersécurité.

• Y.L.P. Il faut également souligner l'apport de la communauté de recherche. Au SnT, nous développons des partenariats bilatéraux avec des entreprises, notamment en cybersécurité, axe stratégique national. Dans ce cadre, j'ai pu observer une incroyable montée en compétences en IA et cybersécurité des entreprises qui ont choisi de collaborer avec nos chercheurs. Ces partenariats contribuent au succès de la transformation digitale du Luxembourg. Le SnT interagit ainsi avec une constellation de partenaires, notre approche scientifique visant à embrasser des problèmes complexes, pertinents pour la recherche et/ou l'innovation, et auxquels les entreprises ne peuvent pas aisément faire face.

Cedric Mauny, *Strategic Advisor Cybersecurity Chez Telindus*

• C.M. Dans ces domaines innovants, il est essentiel de disposer de use cases. Ce sont les entreprises qui apportent ces cas d'utilisation concrets. C'est notamment ainsi que nous pouvons mettre en avant les compétences uniques que l'on trouve au Luxembourg et positionner le Grand-Duché sur la scène internationale. Par exemple pour revenir sur l'IA, nous explorons en cybersécurité la possibilité de générer du trafic réseau qui ressemble à celui que nous observons dans la réalité. L'objectif serait de détecter les schémas malveillants à l'avance, avant même qu'ils ne se dématérialisent. C'est une direction prometteuse mais qui doit encore faire l'objet de nombreux développements et pour laquelle nous avons besoin de chercheurs comme ceux du SnT.

QUE POUVONS-NOUS ATTENDRE DU SNT EN MATIÈRE DE PROJETS DE RECHERCHE INNOVANTS EN 2024 ? ET QUELLE EST LA POSITION DE TELINDUS VIS-À-VIS DES AXES DE TRAVAIL PRIVILÉGIÉS PAR LE CENTRE DE RECHERCHE DE L'UNI ?

• Y.L.T. Le SnT concentre ses efforts de recherche sur quatre axes stratégiques : la FinTech, l'espace, les systèmes autonomes et la cybersécurité, ce dernier domaine bénéficiant actuellement de la plus grande priorité. Malgré des réussites notables dans ce domaine, dont de nombreuses publications au plus haut niveau, nous considérons que la dynamique de la cybersécurité doit encore être développée en synergie avec les acteurs publics et privés du Luxembourg. Nous avons donc décidé de lancer des initiatives ambitieuses, notamment en recrutant des professeurs et des experts de haut niveau dans les domaines de l'IA, de la cybersécurité et de la cyberdéfense.

• C.M. Chez Telindus, nous sommes actifs sur chacun des quatre axes exploités par le SnT. Notre objectif est de fournir aux entreprises des services innovants et de grande qualité. En tant qu'opérateur cloud et telecom, nous disposons d'un vaste maillage de réseaux de tous types au travers desquels nous gérons une quantité considérable de données. Les données sont d'une importance primordiale en matière de cybersécurité, encore plus dans l'open-data economy dans laquelle le Grand-Duché se positionne. En effet, pour détecter des activités malveillantes, anticiper des attaques et y réagir, il est impératif de disposer de données adéquates. In fine, tous nos efforts et nos investissements convergent vers l'objectif de faire du Luxembourg un pôle d'excellence en cybersécurité.

SÉCURITÉ DANS LE CLOUD

UN ENJEU SOUS-ESTIMÉ?

L'une des raisons du succès des solutions cloud demeure dans la sûreté de la mise en œuvre de celles-ci. Travailler dans le Cloud expose cependant à certains risques en matière de sécurité. Parmi les défis auxquels les entreprises sont confrontées, on peut citer la confidentialité des données et la conformité de la sécurité lors de la mise en œuvre de projets cloud. Nous faisons le point sur ces questions avec Audric Lhoas, IT Product Management Team Leader, et Cédric Mauny, Strategic Advisor Cybersecurity, de Telindus.

Lorsque qu'une entreprise se lance dans un projet cloud, tient-elle suffisamment compte de la sécurité ?

• **A.L.** «Les projets cloud soulèvent des préoccupations de sécurité qui ne sont pas toujours prises en compte de manière adéquate. Après la crise sanitaire, de nombreux projets cloud ont vu le jour au Luxembourg, mais la sécurité n'y a, souvent, été intégrée que trop tardivement. Certains projets, tiennent mieux compte de la sécurité, tandis que d'autres, comme les solutions de travail à distance par exemple, la négligent presque complètement».

• **C.M.** En incluant les départements risque, sécurité et conformité dès la conception du projet, on peut intégrer des exigences qui en découlent, y compris juridiques, ce qui permet d'éviter des blocages ultérieurs tout en réduisant les coûts. Cette approche by design garantit la conformité et génère de la confiance aux parties prenantes, y compris aux partenaires, aux investisseurs et aussi aux régulateurs. Négliger l'implication du département sécurité ou ne pas en écouter les exigences et recommandations peut entraîner de sérieuses conséquences pour le business. Les raisons souvent avancées pour un manque de sollicitation proactive sont celles liées à une perception de la sécurité comme un obstacle ou au mieux un manque de sensibilisation aux risques potentiels.

Lorsque vous êtes amenés à mettre sur pied un projet cloud pour le compte d'un client, quel type d'approche de la sécurité préconisez-vous ?

• **A.L.** «Lorsque nous mettons en place un projet cloud pour un client, nous abordons l'aspect sécurité en fonction de deux scénarios distincts. Dans le premier cas, lorsque le client est encore au stade initial du projet, nous privilégions l'approche by design pour intégrer la sécurité dès le départ. Nous tenons compte des recommandations de sécurité, des risques réglementaires et des benchmarks de sécurité tels que les benchmarks CIS, qui sont des normes de bonnes pratiques mondialement reconnues».

« Dans le deuxième scénario, où le projet est déjà réalisé mais où le client n'a pas pris en compte la sécurité de manière adéquate, nous pouvons effectuer un audit pour corriger les lacunes. »

• **C.M.** « Lorsque nous reprenons en main un projet cloud déjà mis en place par un client avec une tierce partie, nous devons d'abord évaluer ce qui a été réalisé. »

« Notre objectif est d'identifier les problèmes et de chercher à combler les lacunes en matière de conformité et de sécurité. La conformité peut être abordée en collaboration avec les équipes d'Audric. Cependant, la sécurité demeure une préoccupation primordiale, car il s'agit de protéger les données, garantir la confidentialité des informations et répondre aux besoins de sécurité tout au long du cycle de vie de la solution. »

« Il est également important de préserver la confiance avec les parties prenantes en démontrant que les besoins de sécurité sont pris en compte. Cependant, l'idéal est d'anticiper et d'intégrer la sécurité dès le début du projet pour éviter de tels rattrapages souvent synonymes de retard ou de coût supplémentaires pour le métier. »

Vous avez l'habitude d'aborder des projets ensemble. Comment articulez vous vos actions respectives ?

• **A.L.** «Nos équipes travaillent en étroite collaboration sur les projets. L'une est responsable de la partie cloud et de la conformité réglementaire tandis que l'autre équipe s'occupe des risques et de la sécurité. Il y a deux aspects majeurs en matière de sécurité : la sécurité initiale, qui est prise en charge par les équipes Cloud, et en Managed Security, qui assure une approche continue et répétitive. »

« Nous ne nous contentons pas de mettre en place la sécurité une seule fois au début du projet. Nous proposons à nos clients des revues de sécurité périodiques – semestrielles ou annuelles - pour s'assurer que l'environnement reste sécurisé et en phase avec les évolutions. Les environnements évoluent et cela peut affecter la criticité des données. Ainsi, nos recommandations incluent également des ajustements au fil du temps pour prendre en compte ces évolutions et maintenir un niveau de sécurité adapté. »

• **C.M.** « J'insiste sur l'importance de suivre en permanence l'évolution de son niveau de sécurité et de conformité par rapport à l'évolution de ses activités métiers et déploiement ICT. Une évaluation aussi bonne soit elle à un instant donné, que ce soit durant le projet ou à sa fin, ne suffit pas pour garantir la sécurité sur la durée. Une des plus grandes erreurs sinon la plus grande serait de supposer que ce qui est parfait au début le restera jusqu'à la fin du cycle de vie de la solution. »

Quels obstacles rencontrez-vous lorsque vous tentez de mettre en place les bonnes pratiques ou les règles de gouvernance liées à la sécurité ?

• **A.L.** «Les grands acteurs du Cloud tels que Microsoft, Google et Amazon sont familiers avec la régulation au Luxembourg et opèrent dans un cadre bien défini. En revanche, lorsque nous travaillons avec des fournisseurs non luxembourgeois, même s'ils sont situés en Europe, ils trouvent souvent intrusif de devoir se soumettre à des procédures de due diligence ou des vérifications préalables. Parfois, ils refusent même de répondre en invoquant le secret. Ce problème concerne principalement les aspects régulatoires, mais il affecte également indirectement la sécurité, car nous ne pouvons pas explorer en profondeur la situation. L'absence de réponse à nos questions complique notre approche de la sécurité car nous ne comprenons pas clairement leur posture vis-à-vis de ces matières et cela crée un véritable problème de confiance».

• **C.M.** «La confiance est un aspect crucial en matière de sécurité. Il est essentiel que les parties prenantes, surtout dans le contexte d'un projet Cloud où les données sont hébergées à l'extérieur de nos frontières, aient confiance dans les fournisseurs de services. Cela implique de s'assurer que le prestataire tiers est et reste fiable dans la durée, qu'il gère efficacement la confidentialité et les droits d'accès en particulier et qu'il est capable de démontrer à tout instant la traçabilité des accès et des mouvements des données. En résumé, la sécurité est intrinsèquement liée à la confiance et joue un rôle essentiel pour garantir la protection et la gestion appropriée des données, en particulier dans un environnement Cloud».

• **C.M.** «Toutes les études, y compris celles menées par le CLUSIL au Luxembourg, indiquent que sécurité et confidentialité sont les principales préoccupations des responsables IT et des CISO. Le RGPD, par exemple, est toujours un élément majeur à prendre en considération. Les évolutions de régulations comme NIS2 ou DORA pour n'en citer que deux, doivent être intégrées pour ce qui est de la continuité et de la résilience de ses activités métiers pour ses partenaires.».

• **A.L.** «Un autre aspect à considérer est le rapport entre le coût de la sécurité et la taille de l'entreprise. Pour certaines petites entreprises, il est difficile de justifier de gros investissements dans la sécurité. D'un côté, les grandes entreprises peuvent mettre en place des mesures étendues, de l'autre, les petites entreprises, parfois composées de seulement quelques employés, renâclent devant un coût qu'elles estiment élevé. Cela peut entraîner des compromis qui ne sont pas toujours les meilleurs.»

En conclusion, le challenge consiste à positionner la «jauge sécurité et compliance" au bon endroit et à s'assurer que les risques soient connus et maîtrisés par les entreprises. Pour cela, il est recommandé de s'appuyer sur des partenaires disposant d'une vue plus large du domaine pour tirer profit de benchmarks et d'informations spécifiques par secteur d'activité. Cela permet de disposer des ressources nécessaires pour être soutenu dans l'implémentation de sa sécurité en toute conformité selon ses propres besoins et son profil de risque.

CYBER SÉCURITÉ

UN IMPÉRATIF STRATÉGIQUE, PLUS QUE JAMAIS

A l'instar de l'environnement économique dont elle garantit le bon fonctionnement, la cybersécurité connaît une transformation rapide qui entraîne une complexification croissante. Yvon Boutry, Tribe Leader Security, nous explique comment Telindus accompagne les entreprises et institutions face à ces nouveaux défis.

QUELLE EST VOTRE PERCEPTION DE L'ÉVOLUTION DU PAYSAGE LUXEMBOURGEOIS CONCERNANT LA CYBERSÉCURITÉ ?

Y.B. En quelques années, nous avons assisté à une profonde transformation des besoins en matière de cybersécurité au sein des entreprises, sur fond d'une forte expansion du marché. Nous évoluons dans un environnement de plus en plus complexe, où toutes les entreprises ont adopté le numérique ou sont en passe de le faire. Cette transformation touche non seulement les infrastructures informatiques et les données, mais également d'autres domaines dans un monde passant au tout numérique.

La sécurité a une influence sur l'ensemble de nos outils de travail et de nos données professionnelles. La protection des systèmes d'information est donc devenue cruciale. À titre d'exemple, lorsque j'ai pris la responsabilité du département Professional Services de Telindus il y a une dizaine d'années, l'équipe ne comptait que cinq ingénieurs. Aujourd'hui, nous sommes trente-deux, et cela pour accomplir les mêmes types de tâches. Cette croissance découle en partie de l'importance accrue accordée à la sécurité au sein des entreprises. Les cyberattaques - comme celles répertoriées récemment au Luxembourg - ont un impact considérable sur les activités des entreprises et peuvent même mettre en question leur pérennité.

Un autre aspect marquant de cette évolution est la complexité. Nous le constatons notamment dans les spécialisations, car un expert en sécurité se doit désormais d'être un professionnel multidisciplinaire. Il doit maîtriser les réseaux, les systèmes, et bien d'autres aspects. La sécurité ne se limite plus à la simple mise en place de pare-feu et de routeurs avec des listes de contrôle d'accès, comme c'était le cas il y a quelques années. Elle s'étend à toutes les couches du système d'information, jusqu'au comportement des applications et des utilisateurs. Cette complexité est amplifiée par la migration vers le Cloud qui a engendré la coexistence de multiples environnements hétérogènes.

QU'APPORTE LE MODÈLE DEVSECOPS ET QUEL RÔLE L'AUTOMATISATION Y JOUE-T-ELLE ?

Y.B. Tout cela complique considérablement le travail de ceux qui sont impliqués dans la mise en œuvre de la sécurité et nécessite de déployer de nouveaux outils et de créer de nouveaux métiers. Il en résulte également un besoin croissant de contrôle, en particulier dans le cas des clouds publics où la confiance – parfois relative - envers les fournisseurs doit être équilibrée par un contrôle accru de la part des entreprises. Or, la complexité croissante, l'accumulation de nouvelles technologies et l'émergence de nouveaux concepts dans le domaine peuvent donner l'impression aux entreprises de ne plus avoir la mainmise sur leur sécurité.

Face à cette complexité, il est essentiel de comprendre les enjeux particuliers à chaque entreprise, d'identifier par exemple les données les plus sensibles et les vulnérabilités spécifiques. Les organisations doivent donc faire des choix stratégiques en matière de sécurité, tout en gérant des budgets qui ne pourront jamais être illimités. En conséquence, il est de plus en plus difficile pour les entreprises de gérer seules leur sécurité.

Cela peut nécessiter de faire appel à des sociétés tierces spécialisées qui ont l'expertise nécessaire pour maintenir un haut niveau de sécurité dans un environnement en constante évolution. C'est précisément là que Telindus apporte un avantage indéniable.

QUELLE RÉPONSE TELINDUS APPORTE-T-ELLE AUX ENTREPRISES EN QUÊTE DE MOYENS POUR RENFORCER LA SÉCURITÉ DE LEURS OPÉRATIONS ?

Y.B. Historiquement, Telindus opérait en tant que prestataire généraliste et intégrateur de solutions. Au fil du temps et en réponse à l'évolution des besoins, nous avons développé un ensemble de "briques de services" destinées à sécuriser nos propres infrastructures, et par extension, à garantir la sécurité des actifs confiés par nos clients.

Aujourd'hui, la sécurité est omniprésente, affectant chaque composant du système d'information. Nous en avons donc conclu qu'il était nécessaire de fédérer nos différentes capacités pour offrir une réponse globale et transversale aux besoins de nos clients.

Offrir une réponse globale signifie que nous pouvons intervenir chez nos clients en leur proposant une gamme complète de services, que ce soit en matière d'infrastructure sécurité, de conseil stratégique en gouvernance, gestion des risques et conformité, d'analyse des failles de sécurité et de remédiation, de tests et simulation d'intrusion, de supervision sécurité, alertes et intervention en cas d'incident via notre équipe de réponse sur incident (CERT/CSIRT). Nous pouvons également les assister sur le plan opérationnel, compte tenu des contraintes que posent à toutes les entreprises la rareté des talents. Notre objectif est de fournir une réponse transversale et intégrée à l'ensemble des aspects de la sécurité, susceptible d'apporter une solution à tous les besoins de nos clients.

COMMENT CONCRÉTISEZ-VOUS CET OBJECTIF ?

Y.B. La stratégie de Telindus en matière de cybersécurité consiste à aider les entreprises à combler les lacunes ou les insuffisances dans leurs capacités en leur fournissant les "briques" qui leur manquent. Cette approche et ses offres associées couvrent l'ensemble du spectre des besoins potentiels. Nous disposons de nombreuses "briques de services" prêtes à l'emploi. Le client a la possibilité de choisir en fonction de sa maturité et de ses besoins spécifiques. Notre volonté est de lui permettre de sélectionner les "briques" qui répondent le mieux à ses attentes.

Pour cela, la clé du succès réside dans une coordination efficace entre nos actions et celles du client. Cela implique de fournir un suivi technique et un accompagnement continu, compte tenu de l'évolution constante du domaine de la sécurité. Le travail en équipe est également essentiel, car une approche transversale et collaborative renforce notre efficacité. Nous disposons de plusieurs équipes d'ingénieurs et de techniciens spécialisés dans différents domaines et nous encourageons une grande collaboration et une communication étroite entre ces équipes. Nous mettons également en place des synergies pour proposer des solutions multidisciplinaires. Par exemple, lors d'une mission d'évaluation des vulnérabilités pour un client, nous faisons appel à des experts en recherche de vulnérabilités, et également à des spécialistes de la défense qui réfléchissent aux enseignements à tirer de cette évaluation. Des consultants seniors sont également impliqués pour dialoguer avec le client et faire évoluer l'infrastructure. Nous proposons des solutions globales qui ne se limitent pas aux technologies ou aux équipes spécifiques, mais qui intègrent une combinaison de compétences pour une réponse plus efficace aux besoins du client.

Nous avons adopté une approche agile et organisée des équipes pluridisciplinaires appelées "squads". Ces squads sont composées d'ingénieurs, de financiers, de logisticiens, ou encore de commerciaux et travaillent sur des sujets spécifiques. Les différentes squads sont rassemblées au sein d'une tribe pour assurer l'opérationnalisation de la stratégie. Cette approche nous permet de structurer nos solutions de manière transversale, de repenser la manière dont nous combinons nos compétences, pour ainsi développer de nouvelles briques de service afin de créer davantage de valeur pour nos clients.

Notre objectif est d'être la référence en matière de sécurité sur le marché luxembourgeois. Cet objectif s'inscrit dans la stratégie globale de Telindus et nous investissons énormément en ce sens.

SÉCURISER LE CYCLE DE DÉVELOPPEMENT APPLICATIF

À l'ère du "tout numérique", l'augmentation de la production de logiciels par des entreprises de tout type élargit d'autant la surface d'attaque potentielle, faisant de la sécurité des applications une priorité absolue. Pour trouver un équilibre entre vitesse et sécurité, les organisations doivent se tourner vers les pratiques DevSecOps. Adapter cette approche, c'est éviter les mauvaises surprises en déploiement et en production, nous explique Tom Leclerc, Head Of Innovation & Software solutions chez Telindus.

POURQUOI EST-IL IMPORTANT DE SÉCURISER L'ENSEMBLE DU CYCLE DE DÉVELOPPEMENT LOGICIEL ?

"L'une des principales raisons est d'éviter les omissions critiques dès le début du processus. Un exemple illustrant cette nécessité est la certification vis-à-vis d'une norme de sécurité ou d'une certification ISO. Souvent, la tentation est de reporter la certification à la phase finale, une fois que le produit est achevé. Cependant, ce choix peut s'avérer problématique, car des éléments importants qui auraient dû être pensés et mis en place tout au long du développement peuvent être omis. Ainsi, pour garantir une certification réussie, il est essentiel de l'aborder en amont, dès les premières étapes".

"L'analyse des risques revêt une importance primordiale. Prendre en compte les risques ne se limite pas à une question de sécurité, mais englobe également la gestion budgétaire associée. Cela suppose d'impliquer toutes les parties prenantes pertinentes, notamment celles ayant un rôle financier dans le projet. Gérer les risques consiste à allouer les ressources adéquates aux aspects les plus critiques du développement, tout en reconnaissant que certains problèmes pourraient ne pas être résolus en raison de contraintes budgétaires. L'analyse des risques agit comme un fil conducteur tout au long du développement, en définissant les besoins en termes de sécurité et en influençant les décisions de conception. Cette approche peut également guider dans les fonctionnalités qui seront intégrées ou exclues en fonction de leur coût et de leur niveau de risque associé".

"De plus, à mesure que le cycle de vie du logiciel progresse, d'autres aspects doivent être pris en compte. Par exemple, lors du décommissionnement d'un logiciel en fin de vie, il est essentiel de mettre en place des mesures pour effacer les données, gérer les archives et prévoir le stockage sécurisé de données essentielles pour de futures utilisations".

"En somme, bien que sécuriser l'ensemble du cycle de développement logiciel puisse sembler complexe, cela se révèle être une démarche essentielle pour garantir la conformité, la qualité et la sécurité du produit final. Chaque étape du processus doit être soigneusement envisagée et traitée, même si certaines questions peuvent sembler évidentes, car une réponse adéquate à chaque questionnement contribue à la solidité globale du logiciel".

QU'APPORTE LE MODÈLE DEVSECOPS ET QUEL RÔLE JOUE L'AUTOMATISATION ?

"Le modèle DevSecOps apporte une synergie entre développement, opérations et sécurité au sein du processus de développement logiciel. L'automatisation y joue également un rôle important".

"Le DevOps, en pratique, implique souvent une automatisation étendue, bien que cela ne soit pas strictement obligatoire. Le concept sous-jacent à DevOps réside dans la collaboration optimale entre les développeurs et les opérations, auquel s'ajoute la sécurité dans le cas du DevSecOps. L'objectif est d'orchestrer ces trois composantes de manière harmonieuse, ce qui se traduit par une agilité accrue et des cycles de mises à jour plus rapides".

"En particulier, l'automatisation joue un rôle essentiel en permettant une collaboration fluide entre des équipes ayant des tâches et des besoins divergents, ainsi que des cycles de vie distincts. Elle contribue à clarifier les rôles entre les équipes de développement et d'opérations. L'automatisation aide également à aborder les problèmes de sécurité en introduisant des vérifications systématiques à chaque étape du processus, du développement à l'exploitation. Ces vérifications incluent l'exécution de tests unitaires fonctionnels et de sécurité, de pentests et d'autres procédures automatisées ou non, permettant d'identifier les failles potentielles et d'assurer la conformité".

"L'émergence de l'Infrastructure -as-Code (IaC) a débloqué la synergie entre le développement et les opérations. Grâce à cette approche, les procédures sont codées, ce qui facilite l'ajout de mesures de sécurité. On peut ainsi s'assurer que le code et l'infrastructure demeurent cohérents entre les versions, et que les règles de sécurité sont respectées. Cette automatisation aide à prévenir les erreurs humaines et assure la mise en place continue de mesures de sécurité.

La plupart des applications modernes reposent sur des API pour interagir avec d'autres logiciels.

QUELS RISQUES LE RECOURS ACCRU AUX API FAIT-IL COURIR AUX ENTREPRISES ? COMMENT PEUT-ON S'EN PRÉMUNIR ?

"Le recours accru aux API peut exposer des processus internes, précédemment limités au système d'exploitation, à des communications réseau ouvertes sur l'extérieur. Cela pourrait permettre des intrusions et des interactions non autorisées avec des parties antérieurement inaccessibles. De plus, la transition vers les API peut entraîner des pertes d'informations sur les types de données et de possibles erreurs de traitement".

"Le recours aux API introduit des avantages, tels que la ségrégation des fonctions et la redondance pour une meilleure résilience. Cependant, ces avantages doivent être abordés en tenant compte du contexte spécifique de chaque logiciel. Des outils comme Docker ou Kubernetes constituent de bons choix en général mais leur utilité dépend du cas d'utilisation".

QU'APPORTE UNE APPROCHE PROACTIVE COMME LA SECURITY BY DESIGN ET QUELS EN SONT LES BÉNÉFICES ?

"Pour se prémunir de ces risques, le Security by Design est crucial. En implémentant la sécurité dès le début, les problèmes futurs sont anticipés et les coûts associés à une implémentation tardive de la sécurité sont évités. Les tests de sécurité, comme les pentests, sont également essentiels, mais doivent être effectués tôt dans le cycle de développement pour identifier les failles potentielles avant l'intégration complète".

A QUELS DÉFIS LES ORGANISATIONS QUI DÉSIRENT SÉCURISER D'AVANTAGE LEURS DÉVELOPPEMENTS APPLICATIFS DOIVENT-ELLES S'ATTENDRE ?

" La sécurité implique un coût substantiel, sans apporter de gains immédiats en termes de rapidité ou de fonctionnalités améliorées. Au contraire, elle peut rendre la gestion plus complexe et ralentir le développement. Il faut considérer la sécurité comme un investissement similaire à une assurance, où l'efficacité est souvent indiscernable tant que tout fonctionne bien".

"Le bon démarrage du processus est capital pour le succès du projet. Une fois que les rôles et responsabilités sont clairs, et que les bonnes pratiques sont établies, la plupart des défis peuvent être gérés efficacement. Il est indispensable d'organiser les équipes de manière cohérente dès le départ, en intégrant dès les premières étapes du développement les exigences de sécurité, la gestion des licences, ainsi que la conformité à des réglementations comme le RGPD. L'équilibre entre la tarification et la protection des données du client est un exemple de la complexité rencontrée. La mise en place de bonnes pratiques est essentielle pour établir un cadre solide".

SMART PROTECTION

PRÉALABLE ET PROLONGEMENT DE LA SÉCURITÉ INFORMATIQUE

Face à un environnement socio-économique sans cesse plus complexe, où les interactions sont de plus en plus nombreuses et fréquentes, Telindus propose des solutions de Smart Protection capables d'améliorer de manière significative la sûreté et la sécurité des opérations courantes des entreprises. Pour détecter et répondre en temps réel aux menaces qui pèsent sur les lieux de travail, les espaces publics et les infrastructures critiques, les solutions de Telindus s'appuient sur des technologies avancées telles que les capteurs, les caméras et les systèmes de contrôle d'accès boostés par l'intelligence artificielle.

"Nos activités se sont développées initialement auprès des infrastructures critiques actives dans les secteurs de l'énergie, de la sécurité publique ou encore des aéroports. Nous étendons aujourd'hui le champ d'application de nos solutions aux secteurs de la finance et de l'industrie en les abordant avec la même expertise développée au sein des infrastructures critiques," explique ***Nicolas Andres,*** Sales Consultant Smart Protection & Unified Collaboration chez Telindus.

Parmi ces solutions, celle bien connue de l'interphone vidéo est un système de surveillance de portes d'entrée qui permet de gérer l'accès à un bâtiment et de communiquer par le biais d'un canal audio/vidéo dédié. Il autorise une communication sans interaction physique, ce qui permet de contrôler et de surveiller l'accès. Il peut également être intégré à d'autres systèmes, tels que des ouvre-portes automatiques, pour faciliter l'accessibilité des visiteurs à mobilité réduite, par exemple. L'interphone vidéo permet l'identification visuelle des visiteurs, réduisant ainsi le risque d'entrée non autorisée.

Le contrôle d'accès, quant à lui, est une méthode de sécurité permettant d'autoriser l'accès physique et virtuel à un espace du moment où des informations d'authentification reconnues sont fournies. Il offre un moyen centralisé et efficace de contrôler l'accès à tous les espaces, éliminant ainsi le besoin de clés physiques pour réduire le risque de perte ou de vol. Le contrôle d'accès contribue également à accroître la productivité en réduisant le temps et les efforts nécessaires pour accéder à un bâtiment.

La protection vidéo augmente la sécurité grâce à l'utilisation combinée de fichiers vidéo et de l'intelligence artificielle pour détecter, analyser et interpréter les données en temps réel. La protection vidéo permet de détecter instantanément

les tentatives et les infractions dans le but d'empêcher les accès non autorisés. Elle fournit également de précieuses informations qui peuvent être utilisées pour améliorer la prise de décision et les performances. Pour faire cela, cette solution intègre des fonctions avancées telles que la détection de mouvement, la reconnaissance faciale et l'intégration avec d'autres systèmes de sécurité, offrant de ce fait des capacités de surveillance améliorées.

"Nous exploitons également notre expertise dans le domaine des technologies intelligentes, en particulier les solutions d'analyse vidéo," ajoute Nicolas Andres. "Nous pouvons ainsi utiliser les images capturées par les caméras pour répondre à différents scénarios. Cela ouvre de nouvelles opportunités comme de détecter des personnes entrant dans des zones interdites, de surveiller des stocks ou bien même d'effectuer des comptages. Notre objectif principal est de soutenir les opérateurs de sécurité. Actuellement, lorsqu'un opérateur supervise un site, il est confronté à plusieurs écrans diffusant une mosaïque d'images, ce qui rend difficile la surveillance de toutes les zones en même temps. Nous augmentons les capacités d'analyse d'images de l'opérateur à l'aide de l'intelligence artificielle et en lui envoyant des alertes basées sur des scénarios préalablement définis. L'avantage de cette approche est de faciliter la prise de décision, car l'opérateur n'est plus seulement dépendant de ses actions et de son attention constante. Le système analyse les données à sa place, ce qui lui permet de se concentrer sur la réaction face à l'incident. Il n'a plus qu'à revoir la décision proposée par l'intelligence artificielle et, si nécessaire, déclencher une intervention."

En déployant les solutions de Smart Protection de Telindus, les entreprises peuvent renforcer la sécurité de leurs espaces et protéger leurs ressources contre les risques de vandalisme ou de vol. Les technologies numériques offrent des vidéos de meilleure qualité et ouvrent la possibilité aux équipes de sécurité d'identifier et de poursuivre les suspects.

"Nos solutions de Smart Protection s'inscrivent dans la stratégie de sécurité globale de Telindus. Elles apportent la couche de protection physique de l'organisation, une première ligne de défense pour la sécurisation des assets d'entreprise. Réciproquement, les capacités de Telindus en cybersécurité permettent de faire en sorte que les défenses physiques ne constituent pas des points d'entrée pour les criminels ou autres personnes mal intentionnées," poursuit Nicolas Andres.

« Afin d'offrir une sécurité complète, l'expertise de Telindus côté réseau peut venir en renfort pour compléter la solution globale au travers de l'implémentation d'éléments de sécurité additionnels sur les couches réseaux et télécommunications fixes ou mobiles " ajoute l'expert.

« En plus de l'aspect sécuritaire, les systèmes de surveillance et de contrôle d'accès peuvent également apporter des données concrètes et pratiques aux responsables de bâtiments concernant l'utilisation effective des lieux. Le contexte actuel est propice aux réflexions sur les solutions dites hybrid-work. Enfin, nos solutions de Smart Protection sont intimement liées à l'environnement Workplace et s'annoncent prometteuses en termes d'innovation »,
conclut ***Nicolas Andres.***

AFTER -WORD

THE BEGINNING OF THE END FOR THE PASSWORD?

Passwords have long been a necessary evil. Once organizations began managing and storing important data, they needed a way to verify what users could access, hence the implementation of a secret key: this was the advent of the password. But attackers soon found ways to guess, steal, bypass, or circumvent password-based security controls.

Today, we know passwords are a not enough secure authentication method. Hackers were quickly able to break passwords because it's easy - people reuse passwords, make them easy to remember ... passwords are vulnerable to social engineering attacks.

Attempts have been made to fix passwords - layering on a multi-factor authentication is the most often used solution - but the password remains the insecure foundation for first-generation of authentication factors because it is still the most cost-effective one. Now it is known and accepted the continued existence of the password, combined with the traditional "castle and moat" network security model, is no more efficient to protect organizations from modern and current attacks.

"'Woof-woof'? That's your idea of a secure password?"

This is where transitioning to a zero-trust security model can help. By following the mantra "never trust, always verify", organizations can limit potential damage by never inherently trusting a device or a user but continuously verifying device level security controls. Instead of the network itself serving as the perimeter, the user's identity becomes the perimeter.

Embarking on a passwordless journey may be a big leap for most businesses, but with a helping hand from your preferred cybersecurity partner, it shouldn't be too hard to jump on the bandwagon and thus ensure that your organization's most valuable assets remain secure and confidential as desired.

Au Vatican, la sécurité, c'est Gustavo.
Au Luxembourg, c'est nous.

Comme Gustavo, nous sommes externes à votre organisation
et nous gérons d'une main de maître votre sécurité informatique.
Avec nos **Managed Security Services**,
vous pouvez vous concentrer sur votre cœur de métier.
Applausi !

www.telindus.lu

SHARE MORE THAN TECHNOLOGY

telindus
CYBERSECURITY