Die Meterspurigen
La voie métrique
A scartamento metrico

RAILplus

Newsletter RAILplus 1 / 2023

NEWS

Dans ce numéro:

- La cybersécurité sur la bonne voie
- Entretien avec Roberto Ferroni, directeur de Ferrovie Luganesi SA

Éditorial de Fabienne Buser

LA CYBERSÉCURITÉ – UN VÉRITABLE DÉFI POUR LES ENTREPRISES

Madame, Monsieur,

Ces dernières années, la sécurité informatique est devenue un enjeu majeur pour les entreprises, quels que soient leur champ d'activité et leur taille. Devenues plus complexes et plus sophistiquées, les cyberattaques ne cessent d'évoluer et de mettre à mal les systèmes en place, même les plus solides. Les défis sont nombreux et les chemins de fer n'en sont pas épargnés.

Pour faire face à cette menace, RAILplus a lancé, en 2020, un appel d'offres pour des services de conseil et créé un centre de compétences ciblé, composé de plusieurs spécialistes en informatique et en cybercriminalité. Son but est de formuler des recommandations basées sur l'analyse des risques et de la maturité cyber, effectuée au préalable au sein des compagnies affiliées. Ces dernières bénéficient donc de clés pour renforcer la sécurité de leurs infrastructures OT (Operational Technologies), pour implémenter dans leur organisation un SMSI (système de management de la sécurité de l'information) et pour sensibiliser leurs collaborateurs au danger de la cybermalveillance. Ces derniers sont par ailleurs mis à contribution lors d'un exercice de gestion de crise dans leur compagnie. Car cela ne fait aucun doute qu'une gestion efficace des cybermenaces peut réduire la probabilité d'une attaque éventuelle et permettre de mieux maîtriser son ampleur.

Face à la hausse de la demande, RAILplus a choisi de proposer ses prestations ainsi que les résultats de ses recherches aux sociétés qui ne font pas partie de son organisation. Pour ce faire et pour de plus amples informations, il suffit de prendre contact avec RAILplus.

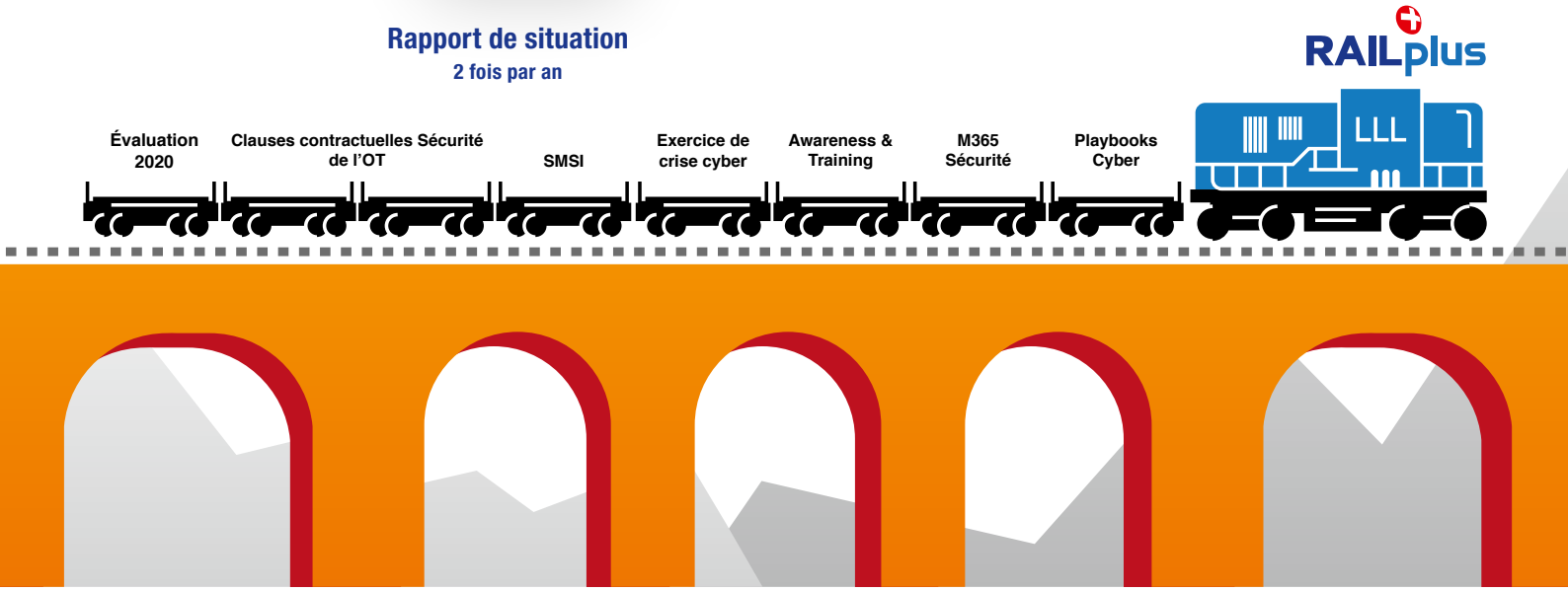
Comme vous pouvez le constater, la cybersécurité est un défi énorme, propulsé au centre des préoccupations ces dernières années. Elle est en outre régulièrement abordée par le groupe de travail Informatique de RAILplus, dont Nicolas Murbach et Urs Siegenthaler en sont les responsables.

Découvrez, dans cette newsletter, leur analyse ainsi que bien d'autres informations sur les activités de RAILplus dans ce domaine. Bonne lecture!

Cordialement,

Fabienne Buser
Assistante de direction, RAILplus SA

Rapport de situation
2 fois par an



LA CYBERSÉCURITÉ SUR LA BONNE VOIE: **LES INITIATIVES DE RAILPLUS**

Depuis 2020, le centre de compétences en cybersécurité de RAILplus offre à toutes les compagnies affiliées des prestations et des mesures dans le but de renforcer leur niveau de maturité. Chaque organisation étant différente, les mesures sont pour la plupart génériques et chaque entreprise est libre de les adopter en y apportant les adaptations nécessaires pour son environnement et ses besoins propres. Nous profitons de cette newsletter pour partager avec vous ce qui a été mis en œuvre depuis trois ans.

Évaluation du niveau de maturité (2020 – 2022)

En 2020, RAILplus a initié une évaluation de la maturité de ses membres en matière de cybersécurité. Cette évaluation a mis en lumière plusieurs domaines clés nécessitant une amélioration, entre autres:

- La gestion des cyberrisques de la chaine d'approvisionnement,
- La sensibilisation et la formation à la cybersécurité,
- Les processus de surveillance et de détection des incidents de sécurité,
- La gestion des incidents de cybersécurité.

À la suite de cette évaluation, huit mesures ont été définies, y compris le rapport d'évaluation, pour renforcer les quatre axes mentionnés précédemment.

En 2022, une mise à jour de l'évaluation a été réalisée afin de mesurer les progrès accomplis par les membres et d'identifier de nouvelles mesures à prendre.

Clauses contractuelles (2021)

RAILplus a mis à la disposition de tous ses membres une annexe de contrat type contenant des clauses relatives à la cybersécurité ainsi qu'une check-list pour les appels d'offres. Cette démarche a permis aux chemins de fer de communiquer ensemble leurs exigences aux fournisseurs et ainsi d'élever leur niveau de sécurité.

Élaboration de recommandations de sécurité pour l'OT (2021 – 2022)

La technologie de contrôle ferroviaire, les infrastructures, le matériel roulant et d'autres domaines du secteur ferroviaire présentent de fortes contraintes (agrément complexe, long cycle de vie, etc.). Cette mesure a permis de proposer des concepts de cybersécurité et des exigences techniques adaptées afin d'augmenter le niveau de cybersécurité de ces systèmes.

Concept SMSI et recommandations (2022 – en cours)

La mise en place d'un SMSI (système de management de la sécurité de l'information) est une exigence de la DE-OCF, art. 5c (Dispositions d'exécution de l'ordonnance sur les chemins de fer). RAILplus a donc élaboré une stratégie qui tient compte des spécificités suivantes:

- L'aspect important de l'OT et des systèmes industriels,
- L'objectif principal de protéger les systèmes critiques qui permettent l'exploitation des trains,
- Les ressources limitées, surtout pour les petits opérateurs,
- Les différences de culture et la sensibilité à la thématique de la sécurité cyber au sein des différents groupes de l'entreprise (IT; OT: infrastructure, installations de sécurité, matériel roulant, etc.).

Exercice de gestion d'une crise cyber (2022 – en cours)
Depuis la fin de l'été 2022, RAILplus accompagne les compagnies dans la préparation et la réalisation d'un exercice de gestion d'une crise afin d'évaluer leur capacité à faire face à un incident cyber majeur et de renforcer leur résilience. Pendant cet exercice d'environ trois heures, les participants sont confrontés à un scénario réaliste impliquant des stimuli fictifs, tels que des e-mails, des publications sur les réseaux sociaux, des articles de presse, etc. L'objectif est de simuler une situation de crise et d'évaluer les mesures prises par les participants. Un rapport contenant les points positifs, mais aussi les axes d'amélioration est ensuite transmis aux entreprises concernées.

Il est important de noter que ces exercices n'ont aucun impact sur l'infrastructure IT/OT ou les opérations ferroviaires car il ne s'agit que de simulations.

Awareness & Training (2021 – en cours)
Trois formations ont été organisées, en allemand et en français, sur les clauses contractuelles et les exigences de base en matière de cybersécurité ainsi que sur le catalogue des risques et le concept SMSI.

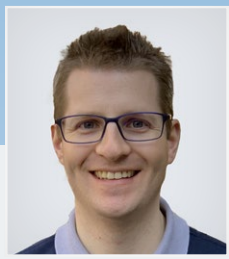
En complément, un e-learning dédié au SMSI et à la future directive de l'OFT est en cours d'élaboration et sera intégré sur la plateforme Moodle dans le courant de l'année 2023. Son but sera de sensibiliser les chefs de projets et les cadres sur les enjeux de la cybersécurité.

Par ailleurs, consciente de la menace liée au phishing et au social engineering, RAILplus met à disposition l'outil Hoxhunt pour entrainer régulièrement les utilisateurs. Cet outil a été présenté aux responsables informatiques de chaque compagnie et est actuellement en phase de test (Proof of Concept) parmi plusieurs membres.

Sécurité MS365 (2023 – en cours)
L'utilisation de Microsoft 365 se généralise et la sécurité d'une telle plateforme devient de plus en plus importante. RAILplus propose donc un ensemble de bonnes pratiques en termes de sécurité afin d'optimiser l'utilisation des licences (E3, E5) et d'améliorer la sécurité globale. Une formation sera également organisée sous la forme d'une présentation et d'une série de questions/réponses.

Playbooks Cyber (2023 – en cours)
Lors d'incidents de cybersécurité, il est crucial de suivre certaines étapes bien définies pour faciliter la réponse et minimiser les dégâts. Ainsi, RAILplus va fournir aux chemins de fer des modèles de marche à suivre (playbooks) pour différents types d'incidents (DDoS, ransomware, etc.). Ces modèles seront adaptables à la situation et aux spécificités de chaque chemin de fer afin de garantir une réponse plus efficace à l'incident.

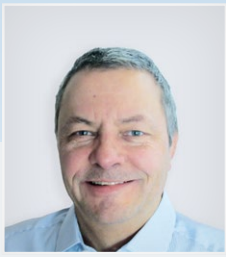
Rapport de situation
Deux fois par an, un rapport de situation est mis à la disposition des membres, dans lequel figurent l'état d'avancement de chaque mesure ainsi qu'un aperçu des menaces cyber dans le domaine ferroviaire et des évolutions en matière de cybersécurité.



NICOLAS MURBACH

Responsable Informatique, Compagnie du Chemin de fer Montreux Oberland bernois SA, responsable du groupe de travail Informatique en Suisse romande

Le groupe de pilotage se rencontre au minimum une fois par mois, notamment pour répondre aux actualités en matière de cybersécurité. Les différentes compétences et expériences de ses membres dans ce domaine garantissent une bonne alchimie au sein du groupe. En outre, cela nous permet, en tant que responsables des groupes de travail Informatique de Suisse alémanique et de Suisse romande, de gérer les projets et d'informer les groupes de travail sur l'état d'avancement des travaux. Par ailleurs, nous entretenons des échanges réguliers avec l'OFT, les CFF, l'UTP et le Centre national pour la cybersécurité (NCSC), qui deviendra, le 1er janvier 2024, le nouvel Office fédéral de la cybersécurité.



URS SIEGENTHALER

Responsable Informatique (CIO), Jungfraubahnen Management AG, responsable du groupe de travail Informatique en Suisse alémanique

Le groupe de travail Informatique de RAILplus a pris conscience, il y a plusieurs années, de l'urgence de réagir ensemble à la menace toujours plus grande des cyberattaques. Afin d'exploiter les nombreuses synergies et de répondre au besoin des compagnies affiliées de bénéficier de prestations dans ce domaine, RAILplus a mis sur pied un centre de compétences ciblé.
Les recommandations et les modèles sont très utiles et aident les chemins de fer à répondre aux exigences toujours plus élevées. Il convient également de mentionner les exercices de gestion d'une crise cyber menés au sein des compagnies affiliées. Ces derniers permettent de mettre en évidence les vulnérabilités et de formuler des recommandations ciblées.

RAILplus a par ailleurs créé le centre de compétences nextRAILplus dans le domaine de la digitalisation de l'exploitation ferroviaire. Vous trouverez ici toutes les informations à ce sujet:

CHIFFRES CLÉS
Ferrovie Luganesi SA

Nombre de collaborateurs:	49 personnes, effectif moyen de 45,84
Longueur du réseau:	12.260 km
Longueur de la voie ferrée:	14.958 km
Point le plus bas:	273.541 (au km 7.803, PL 3 Stazione Agno)
Point le plus haut:	350.843 (au km 1.710, à peu près à mi-chemin du quai de la gare de Laghetto)
Écartement des rails:	1000 mm
Déclivité la plus forte:	29.7 o/oo (entre le km 6.520 et le km 6.680 – et entre le km 10.000 et le km 10.170)
Recettes provenant du trafic:	CHF 4.5 millions en 2022

ENTRETIEN AVEC **ROBERTO FERRONI**

Directeur de l'entreprise Ferrovie Luganesi SA

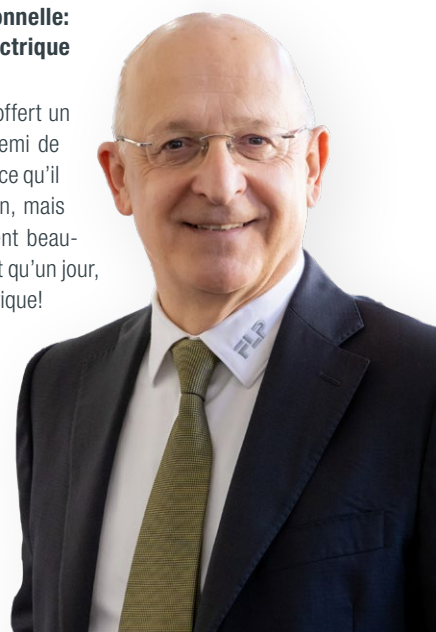
Monsieur Ferroni, où se situe, aujourd'hui, l'entreprise FLP?
Bien qu'elle ait soufflé ses 110 bougies en 2022, l'entreprise FLP connaît une nouvelle jeunesse ces dernières années. Après avoir participé, ou si j'ose dire déterminé, le développement et la croissance du Malcantone depuis le début du 20e siècle, elle s'apprête une nouvelle fois à être la protagoniste d'un changement révolutionnaire dans la mobilité du sud du Tessin. Son importance pour le transport local ne fait aucun doute, car non seulement elle relie de manière efficace les agglomérations entre elles, mais elle permet également d'accéder au réseau ferroviaire national, ce qui facilite les relations économiques et sociales. Chaque année, sur les 12,25 km de la ligne qui relie Ponte Tresa à la gare de Lugano, le FLP transporte en moyenne plus de 2,5 millions de passagers, un chiffre extrêmement important pour une région qui a toujours souffert du trafic routier privé, en particulier de celui provenant de l'Italie voisine.
L'année 2021 a constitué une étape importante pour le FLP avec l'arrivée des nouvelles rames Tramlink, qui ont remplacé les rames historiques Mandarinli, lesquelles ont, durant plus de 40 ans, accueilli des générations entières de clients fidèles. En mars dernier, une autre étape importante a été franchie avec l'approbation des plans du RTTL (le projet de réseau de tramway de Lugano, dont je parle plus en détail ci-dessous). Aujourd'hui, le FLP peut compter sur l'engagement d'une cinquantaine de collaborateurs, qui assurent le bon fonctionnement de l'entreprise, tout en gérant l'exploitation, les relations avec nos clients, les 9 trams-trains et tous les aspects techniques du réseau.

Quels sont vos plus grands défis pour ces cinq prochaines années?
Comme mentionné précédemment, le FLP fait partie intégrante d'un projet cantonal qui marquera une nouvelle évolution de la mobilité dans la région: le projet Rete Tram del Luganese (RTTL).
Ce nouveau réseau, sympathiquement appelé «La Metropolitana del Luganese», contribuera à redéfinir l'agglomération urbaine de Lugano, en reliant le Basso Vedeggio, le Malcantone et le centre-ville comme jamais auparavant. La fréquence des courses (toutes les cinq minutes sur certaines lignes) et la réduction considérable de la durée des trajets en feront l'option de mobilité la plus avantageuse. Selon les plans, ce projet deviendra réalité en 2030. Le premier défi du FLP pour ces prochaines années sera certainement de continuer à développer et à perfectionner les Tramlink pour les rendre encore plus efficaces.

Qu'a apporté votre adhésion à RAILplus dans le passé?
Le fait de pouvoir bénéficier de l'expérience et du savoir-faire des autres membres nous a motivés à rejoindre RAILplus. Bien que de petite taille, notre entreprise est impliquée dans divers projets de grande envergure. Par conséquent, faire partie de RAILplus nous permet d'entretenir des échanges, d'élargir notre vision et d'explorer de nouvelles perspectives grâce à l'expérience des autres entreprises, ainsi que de bénéficier, par le biais du groupe des achats stratégiques, de conditions financières avantageuses.

Quelles sont vos attentes à l'avenir envers RAILplus?
Comme prévu, faire partie de RAILplus constitue une grande opportunité pour notre entreprise, mais également une valeur ajoutée pour l'ensemble du secteur ferroviaire. Pouvoir compter sur une organisation en mesure de répondre aux besoins de ses membres et d'entretenir une coopération entre les chemins de fer suisses à voie métrique, c'est ce qui, à mon avis, peut contribuer au développement du secteur dans son ensemble, à son innovation et à son efficacité. Il est rassurant pour nous de savoir que les besoins d'une entreprise comme le FLP peuvent être représentés à Berne grâce à l'intercession et à notre coopération avec RAILplus. Il en va de même dans le domaine de la formation: grâce à RAILplus, nos responsables profitent d'un précieux échange d'expériences, ce qui, nous le savons, est un gage de qualité et de modernité.

Pour terminer, une question personnelle: combien de mètres votre train électrique mesure-t-il chez vous?
À l'âge de 6 ans, mes parents m'ont offert un train en bois d'environ un mètre et demi de long. Au début, j'ai été un peu déçu parce qu'il ne bougeait pas sans mon intervention, mais j'ai vite changé d'avis et j'ai finalement beaucoup joué avec ce train, me promettant qu'un jour, j'en aurais un bien plus long et électrique! Aujourd'hui, je peux dire que j'ai réalisé ce rêve, et ce, bien au-delà de mes espérances de l'époque.

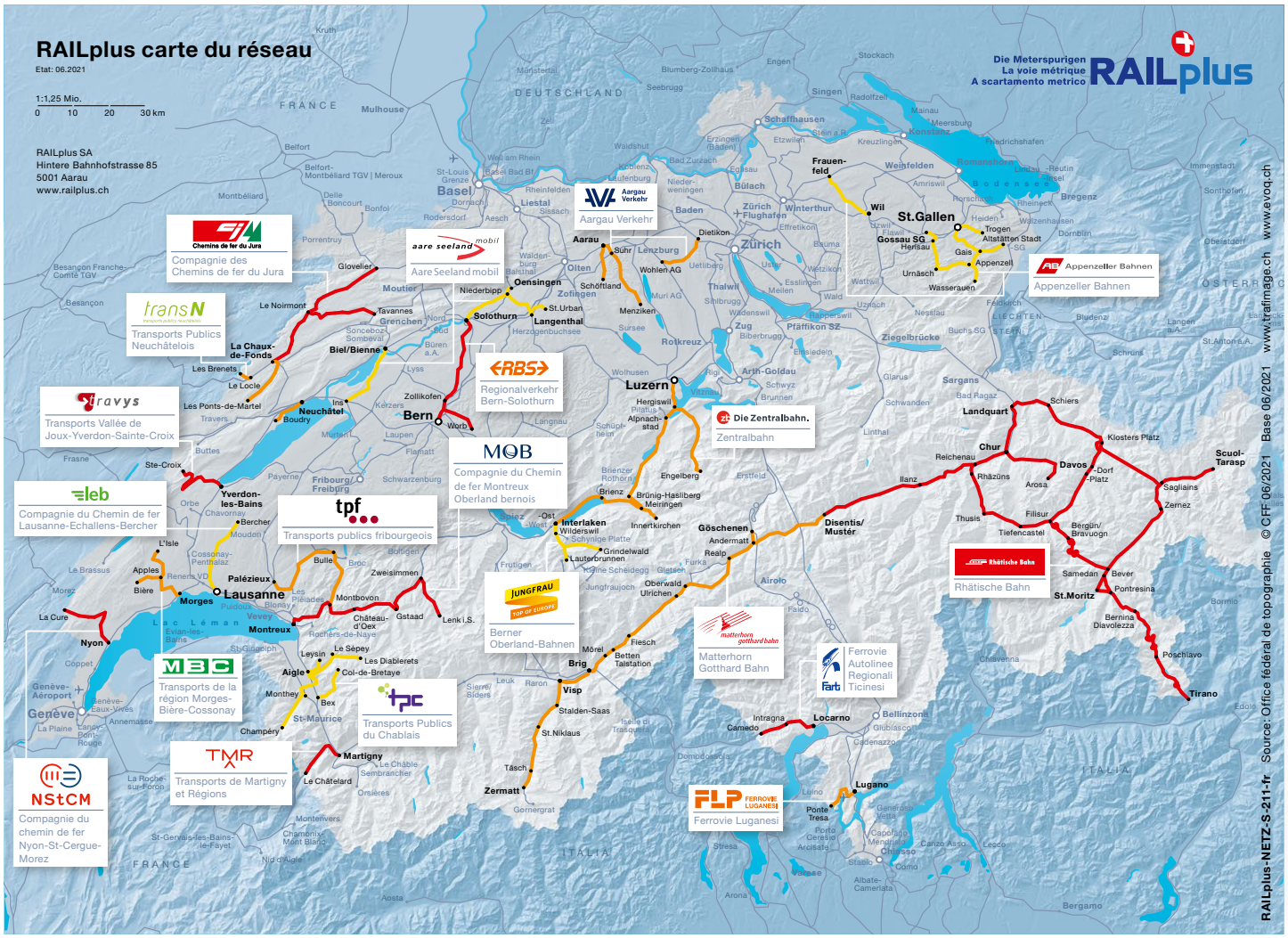


CYBERSECURITY:
UNA VERA SFIDA PER LE AZIENDE

Negli ultimi anni, la sicurezza informatica è diventata un problema importante per le aziende, indipendentemente dal loro settore di attività o dalle loro dimensioni. Gli attacchi informatici sono diventati più complessi e sofisticati e si evolvono costantemente, minando anche i sistemi più solidi. Le sfide sono molte e le ferrovie non sono immuni.

Per far fronte a questa minaccia, RAILplus ha creato nel 2020 un centro di competenza specifico, composto da diversi specialisti in informatica e cybercriminalità. L'obiettivo è formulare raccomandazioni basate sull'analisi preventiva dei rischi e della maturità informatica delle aziende affiliate. A queste ultime vengono così forniti gli strumenti necessari per rafforzare la sicurezza delle loro infrastrutture OT (Operational Technologies), per implementare un ISMS (Information Security Management System) nella loro organizzazione e per sensibilizzare i loro collaboratori sul pericolo del cyber-malware. Questi ultimi sono anche coinvolti in un esercizio di gestione della crisi nella loro azienda. Una gestione efficace delle minacce informatiche può ridurre, senza ombra di dubbio, la probabilità di un possibile attacco e permettere di controllarne meglio la portata.

In seguito alla crescente domanda, RAILplus ha deciso di proporre i suoi servizi e i risultati della ricerca a società esterne alla sua organizzazione. Per ulteriori informazioni, si prega di contattare RAILplus.



MENTIONS LÉGALES

Éditeur: RAILplus SA | Hintere Bahnhofstrasse 85 | 5001 Aarau | info@railplus.ch | www.railplus.ch | **Directeur:** Joachim Greuter
Tirage: 1500 exemplaires en allemand, 900 exemplaires en français | **Mise en page:** Top Line Marketing | **Fréquence de parution:** deux fois par année