

Discussion du panel dans le cadre des Swiss Cyber Security Days 2024, 21 février 2024

Chers membres,

Début novembre 2023, l'Office fédéral de la cybersécurité (à l'époque encore le Centre national de cybersécurité) a enregistré un nouveau record avec plus de 2000 cyber incidents annoncés en une semaine. Comme il ne s'agit que des incidents déclarés, il reste un chiffre noir concernant les cyberattaques réellement survenues. L'annonce de ce nouveau record doit donc être considérée comme un appel au réveil : Le renforcement de la cyber-résilience en Suisse est d'une importance capitale.

En effet, en tant que pays le plus innovant du monde, la Suisse représente une cible particulièrement attrayante pour les cyberattaques. De nombreuses entreprises et organisations ont entre-temps reconnu le danger. La Confédération a elle aussi décidé de procéder à d'importants changements institutionnels et législatifs au début de l'année 2024.

- Quels effets et changements peut-on attendre de la **création du Secrétariat d'État à la politique de sécurité (SEPOS)** et de l'**Office fédéral de la cybersécurité (BACS)** pour l'architecture de la cybersécurité en Suisse ?
- Comment le **BACS** fait-il face à l'hétérogénéité des menaces provenant du cyberspace ?
- Comment la nouvelle **loi sur la sécurité de l'information (LSI)** modifie-t-elle les **exigences minimales** en matière de **sécurité de l'information de la Confédération** et quelles en sont les **conséquences** pour les **autorités**, les **cantons** et les **tiers** ?
- Comment fonctionnent la **répartition des tâches** et la **subsidiarité** dans le domaine cybernétique entre la Confédération, les cantons et les communes ? Quelle est l'importance du **Réseau national de sécurité (RNS)** ? Qui coordonne les différents services et organes ? Qui est responsable des domaines de la cybersécurité, de la cybercriminalité et de la cyberdéfense ?
- Dans quelle mesure le **secteur privé** a-t-il la responsabilité d'augmenter sa cyber-résilience et comment les petites entreprises peuvent-elles augmenter leur résistance avec des moyens limités ?
- Que faut-il faire dans le domaine de la **prévention**, de la **sensibilisation**, de la **déstigmatisation** et de la **formation** en matière de cybermenaces auprès des autorités, des administrations, des entreprises et des particuliers ?

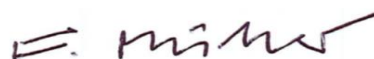
Nous vous invitons à discuter de ces thèmes et défis importants avec des experts lors du **16e FSS Security Talk** dans le cadre des Swiss Cyber Security Days.

Nous nous réjouissons de votre participation !

Avec nos meilleures salutations



Hans-Jürg Käser
Président
FORUM SÉCURITÉ SUISSE (FSS)



Fredy Müller
Directeur général
FORUM SÉCURITÉ SUISSE (FSS)

Programme

15:00 Table ronde et questions-réponses

Invités du panel :

Martin von Muralt, Délégué pour le Réseau national de sécurité RNS

Florian Schütz, Directeur de l'Office fédéral de la cyber-sécurité

Tobias Schoch, Chief Security Officer, AXA Suisse

Maja Riniker, Conseillère nationale (PLR, AG) et membre du groupe parlementaire Cyber

Gerhard Andrey, Conseiller national (Verts, FR) et membre du groupe parlementaire Cyber

Modération :

Fredy Müller, Directeur général de FSS

Inscrivez-vous maintenant !

Inscription à : www.forum-sicherheit-schweiz.ch/kommende-talks | +41 (0)44 533 04 00 | ou : sekretariat@forum-sicherheit-schweiz.ch

Grâce à notre partenariat, profitez d'une offre exclusive pour les membres de la FSS et achetez la carte journalière pour le 21 février au prix fortement réduit de 153 CHF seulement au lieu de 510 CHF.

Nous remercions nos partenaires événementiels et nos partenariats annuels !



FORUM SÉCURITÉ SUISSE

c/o MUELLER Consulting & Partner
Gemeindestrasse 48
CH-8032 Zürich

Téléphone : +41 44 533 04 00
sekretariat@forum-sicherheit-schweiz.ch