Forum neuchâtelois **sur la cybersécurité**

>cnci

01

LA CYBERMENACE DANS LES ENTREPRISES

COMMENT ANTICIPER ?

La meilleure des défenses est l'anticipation, soyez plus intelligent que les hackers ! Ne sous-estimez pas l'impact financier, technique et humain d'un cyber-incident. Votre gestion du risque cyber peut passer notamment par des mesures techniques/informatiques, des processus et des politiques clairs et renforcés ainsi que de la formation du personnel. Combiner ces mesures à une cyberassurance vous permettra une défense à 360°.

Nos recommandations

- Ne restez pas inactif, soyez proactif et préparez un plan d'action en cas d'incident.
- Protégez-vous contre l'impact financier non négligeable des cyber-incidents.
- Sous pression, pas de décision hâtive : vérifiez avant d'agir.

02

ATTENTION AUX PIRATES !

Quatre grands profils de pirates se dégagent : les cybercriminels motivés par l'argent, les espions d'État ou industriels, les hacktivistes dans des logiques de guerre numérique et les menaces internes. Des entreprise et organisations suisses de toutes tailles font l'objet d'attaques.

Comprendre les motivations de ces pirates ainsi que leurs méthodes est essentiel pour mieux s'en protéger.

Nos recommandations

- Contrôlez les accès aux données sensibles, surtout en cas de départ d'un collaborateur ou de conflit interne.
- Évaluez régulièrement vos fournisseurs et sous-traitants sur le plan cyber.
- Formez vos équipes aux risques liés au phishing et à l'ingénierie sociale.

UN GRAND MERCI AUX INTERVENANTS

police NEUCHÂTELOISE · ello · UDITIS by Sequotech · VAV · ELCASecurity · baloise · navixia · Cyber-Conseil

03

DEEPFAKE ET DARK WEB : *ENTRE MYTHES ET RÉALITÉS*

Les organisations sont confrontées à des menaces de plus en plus sophistiquées ; les deepfakes et le dark web constituent aujourd'hui des vecteurs de risques spécifiques : usurpation d'identité, fraude financière, cyberattaques, atteinte à la réputation ou fuite de données sensibles.

Nos recommandations

- Vérifiez toujours par un second canal toute demande inhabituelle ou urgente, même si elle semble provenir d'un dirigeant.
- Protégez les accès sensibles avec une authentification multifacteur (MFA) et une gestion rigoureuse des identifiants.
- Mettez en place une veille et une surveillance du dark web afin de détecter rapidement d'éventuelles fuites de données.

04

FORMATION DES COLLABORATEURS AUX CYBER-RISQUES

Il est essentiel de former ses collaborateurs à reconnaître les cyber-risques, car la plupart des attaques réussies comportent aujourd'hui une composante sociale. Un utilisateur sensibilisé renforce au quotidien la protection de toute l'infrastructure. Mais, pour que la formation déploie tous ses effets, il convient de s'appuyer sur quelques principes fondamentaux. Ils sont simples, pragmatiques, et ils font toute la différence.

Nos recommandations

- Définissez le périmètre de la formation en fonction de votre réalité.
- Tenez compte de la charge de travail existante. Pensez long terme.
- Communiquez. Instaurez un climat de formation bienveillant.

>Informer >Sensibiliser >Soutenir

L'organisation du second forum neuchâtelois sur la cybersécurité a permis à la CNCI d'informer les entreprises et PME de notre canton sur cette problématique, ainsi que de les sensibiliser et de les soutenir par rapport à un phénomène qui peut paralyser des petites comme des grandes sociétés. La CNCI remercie les onze intervenants, issus de l'entrepreneuriat et d'institutions étatiques, de leur précieuse contribution à l'organisation de cette manifestation.

Au cœur de l'économie

>cnci
Chambre neuchâteloise du commerce et de l'industrie
Rue de la Serre 4
2000 Neuchâtel
Tél. 032 727 24 10
cnci@cnci.ch
www.cnci.ch