Le SIEN

ne.ch
RÉPUBLIQUE ET CANTON DE NEUCHÂTEL
DÉPARTEMENT DE LA FORMATION, DE LA DIGITALISATION ET DES SPORTS (DFDS)

QUE FAIRE EN CAS DE CYBERATTAQUE ? (dirigeants)

Méthodologie de gestion des cyberattaques pour les dirigeants des partenaires conventionnés avec le SIEN.

1 PREMIERS RÉFLEXES

Alertez immédiatement le SIEN au 032 88 91111 ou au 032 71 7811 afin qu'il prenne en compte l'incident.

Isolez les systèmes attaqués afin d'éviter que l'attaque ne puisse se propager à d'autres équipements en coupant toutes les connexions au réseau local (introduction IT, WIFI), ne pas allumer les ordinateurs éteints.

Constituez une équipe de gestion de crise afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique...).

NE PAYEZ PAS DE RANÇON !

Car vous encourageriez les cybercriminels à chercher à vous attaquer à nouveau et financeriez leur activité criminelle tout en n'ayant aucune garantie qu'ils tiendront leur parole.

Tenez un registre des évènements et actions réalisées tirer les enseignements de l'incident a posteriori et mettre à les traces à disposition des enquêteur.

Préservez les preuves de l'attaque : messages reçus, appels téléphonique suspect..

2 PILOTER LA CRISE

Mettez en place des solutions de secours pour pouvoir continuer d'assurer les services indispensables. Activez votre plans de continuité et de reprise d'activité (PCA-PRA) si vous en disposez.

Déclarez le sinistre auprès de votre assureur qui peut vous dédommager .

Listes de mes contacts clés internes et externes:

Alertez votre banque au cas où des informations permettant de réaliser des transferts de fonds auraient pu être dérobées.

Déposez plainte avant toute action de remédiation en fournissant toutes les preuves en votre possession.

Le SIEN identifie l'origine de l'attaque et son étendue afin de pouvoir corriger ce qui doit l'être et éviter un nouvel incident.

Notifiez l'incident au PPDT-JUNE dans les 72h si des données personnelles ont pu être consultées, modifiées,détruites ou volées par les cybercriminels.

Gérez votre communication afin d'informer avec le juste niveau de transparence vos administrés, clients, collaborateurs, partenaires, fournisseurs, médias...

Le SIEN

ne.ch
DÉPARTEMENT DE LA FORMATION, DE LA DIGITALISATION ET DES SPORTS (DFDS)

3 SORTIR DE LA CRISE

Le SIEN effectue une remise en service progressive et contrôlée après s'être assuré que le système attaqué a été corrigé de ses vulnérabilités et en en surveillant son fonctionnement pour pouvoir détecter toute nouvelle attaque.

Tirez les enseignements de l'attaque et définissez les plans d'action et d'investissements techniques, organisationnels, contractuels, financiers, humains à réaliser pour pouvoir éviter ou a minima pouvoir mieux gérer la prochaine crise.

PRENEZ EN COMPTE LES RISQUES PSYCHOLOGIQUES

Une cyberattaque peut engendrer une surcharge exceptionnelle d'activité et un sentiment de sidération, d'humiliation, d'incompétence voire de culpabilité susceptible d'entacher l'efficacité de vos équipes durant la crise et même au-delà.

CONTACTS UTILES

Conseils et assistance

Centre national pour la cybersécurité

https://www.ncsc.admin.ch/ncsc/fr/home.html

Notification de violation de données personnelles

Préposé à la protection des données et à la transparence

https://www.ppdt-june.ch/

Police Neuchâteloise: 032 889 90 00

Suivez les consignes du SIEN https://partenaires.ne.ch et https://neinfo.ch