Toujours une longueur d'avance : Rester informé et réagir rapidement aux points faibles

Dans le paysage numérique actuel en constante évolution, les entreprises de toutes tailles sont constamment exposées aux cyber-risques. Selon la Cybersecurity Infrastructure Security Agency (CISA), 50% des failles de sécurité connues et exploitées le sont dans les deux jours suivant leur découverte et 75% dans un délai inférieur à un mois. Une gestion active des vulnérabilités est indispensable pour pouvoir agir rapidement et remédier à la situation avant que des activités malveillantes ne pénètrent et ne se propagent dans le réseau d'une entreprise.

La détection dynamique des vulnérabilités de Chubb

Grâce à notre programme Vulnerability Management Outreach, notre équipe Cyber Intelligence surveille, scanne et identifie régulièrement les vulnérabilités et les nouvelles menaces critiques afin de protéger nos assurés. Les cyber-assurés qui s'inscrivent pour recevoir des alertes sont informés par :

Programme de sensibilisation - Une notification proactive est envoyée lorsque des vulnérabilités critiques connues sont découvertes dans l'environnement système et qu'elles ont une forte probabilité d'être exploitées.

- Une première notification est envoyée par e-mail, détaillant le risque et les mesures nécessaires pour y remédier.
- Les suivis sont effectués par e-mail et par appels téléphoniques.

Alertes rapides - Elles sont envoyées par e-mail aux cyber-assurés lorsque de nouvelles vulnérabilités à forte probabilité d'exploitation sont découvertes et pourraient avoir un impact sur l'environnement système.

- Un e-mail contenant des informations sur la nouvelle menace est généralement envoyé dans les 24 heures.

Solutions supplémentaires pour la gestion des vulnérabilités

En plus de notre programme de sensibilisation à la gestion des vulnérabilités, tous les cyber-assurés Chubb peuvent s'inscrire aux cyber-services gratuits suivants :

- **Surveillance externe des vulnérabilités** - En coopération avec BitSight, les assurés peuvent surveiller quotidiennement les cyber-risques de leur entreprise via une plateforme qui met en évidence les points forts et les vulnérabilités potentielles à l'aide d'indicateurs spécifiques et offre un aperçu de la sécurité de leur organisation.

Pour vous inscrire au programme Chubb Vulnerability Management Outreach et pour obtenir plus d'informations sur Chubb Cyber Services, veuillez consulter le site suivant : www.chubb.com/ch-fr/switzerland-cyber-services.html

Programme de sensibilisation aux vulnérabilités Chubb

Questions fréquentes sur l'alerte de signalement

FAQ générales

Quel est l'objectif du Programme de sensibilisation aux vulnérabilités de Chubb ?

- Il vise à informer les organisations de leur exposition à des vulnérabilités qui présentent des risques élevés et autres erreurs de configuration graves (ports ouverts, infection par des logiciels malveillants, etc.). Chubb a adopté cette approche afin d'alerter ses assurés à identifier et à remédier aux problèmes liés à la connexion à Internet que notre équipe spécialisée dans la veille sur les menaces a classés comme des expositions à des risques élevés et de les accompagner dans cette démarche. Ainsi, chacune des vulnérabilités que nous identifions peut être et sera identifiée en fonction des auteurs de la menace. En outre, la liste des vulnérabilités que Chubb recherche est considérée comme hautement exploitable si elle se retrouve dans la nature.

Pourquoi Chubb m'alerte-t-elle en cas de découverte de vulnérabilités dans mon environnement ?

- Cette alerte constitue une composante essentielle de la relation symbiotique qui existe entre Chubb et nos assurés. Nous fournissons des services d'ingénierie du risque à nos assurés dans le monde entier depuis plus de cent ans, ce qui fait de nos assurés de meilleurs gestionnaires du risque, et de Chubb un meilleur assureur. Il en va de même dans le domaine de la cybersécurité. Puisque nous priorisons les vulnérabilités qui engendrent des pertes et/ou figurent sur des listes de veille sur les cybermenaces présentant des risques élevés que nous découvrons dans l'environnement de nos assurés, la réduction de l'exposition à ces vulnérabilités constitue une priorité.

Ces alertes ont-elles un impact sur mes garanties ?

- Non. Toutefois, une réticence à prendre des mesures visant à remédier à ces vulnérabilités prioritaires peut avoir une incidence sur la souscription de votre contrat par la suite. Si nous constatons, par exemple, que ces vulnérabilités persistent et que nous ne recevons aucune réponse ou ne constatons aucune action de la part d'un assuré, nous pouvons envisager de ne pas renouveler son assurance.

S’agit-il d’un test d’intrusion ?

- Non, il ne s’agit pas d’un test d’intrusion. Aucune analyse active ou tentative de s’introduire dans votre environnement n’est réalisée. Ce processus utilise des plateformes d’analyse active externes qui s’appuient sur une combinaison de veille open source (OSINT) et d’analyse passive. Cette analyse passive n’est pas intrusive et constitue un outil sûr pour identifier les actifs connectés à Internet et les éventuelles vulnérabilités ou erreurs de configuration connexes.

FAQ relatives aux signaux d’alerte

Pourquoi est-ce que je reçois une alerte ?

- Vous recevez cette alerte car vous vous êtes inscrit au Programme de sensibilisation aux vulnérabilités de Chubb, proposé à l’ensemble de nos assurés en complément de leur contrat d’assurance Cyber. Elle porte soit sur une vulnérabilité exploitée connue (VEC), soit sur toute autre atteinte grave à la cybersécurité qui a été détectée grâce aux outils d’analyse externes non intrusifs, tels que BitSight et Security Scorecard. Cette alerte inclut des informations que l’équipe informatique de l’assuré peut utiliser pour identifier l’actif exposé et remédier à la situation.

Et si je ne comprends pas ces alertes ?

- L’équipe Veille Cyber de Chubb se fera un plaisir d’évoquer ce processus et de fournir des informations détaillées concernant cette alerte à l’un des membres de votre organisation. Vous pouvez également la transmettre à votre responsable de la sécurité informatique interne ou à un prestataire de services gérés tiers qui supervise votre environnement pour toute clarification et/ou analyse.

Je ne sais pas de quoi il retourne ou ce qu’il faut faire à ce sujet, pouvez-vous m’aider ?

- Oui, vous pouvez demander à ce que l’équipe de conseil en risque cyber de Chubb vous recontacte en écrivant à Cyber@chubb.com
- Pensez à bien ajouter un commentaire indiquant que vous avez reçu une alerte de vulnérabilité et que vous souhaitez en discuter.

Ce n’est pas mon adresse IP. Une action est-elle requise ?

- Veuillez transmettre cette alerte à Cyber@Chubb.com en précisant les adresses IP erronées et nous mettrons à jour nos dossiers en indiquant qu’elles concernent un actif non assuré. Si vous êtes intéressé, l’équipe de conseil en risque cyber de Chubb peut donner des instructions à votre équipe informatique afin de soumettre une demande concernant ces conclusions via Bitsight ou Security Scorecard et ainsi éviter de futures alertes automatisées concernant ces IP erronées.

Ce n’est pas mon domaine.

- Veuillez écrire à Cyber@Chubb.com en confirmant le domaine exact et Chubb veillera à ce que votre contrat soit mis à jour sur cette base. Nous mettrons ensuite à jour nos dossiers afin d’indiquer que la vulnérabilité concerne un actif non assuré et clôturerons le dossier associé.

Tous les cyber-services sont susceptibles aux changements. Les modifications apportées à l'offre de prestations, sont indiquées sur le formulaire web local des cyber-services. Il est la responsabilité des preneurs d'assurance de vérifier leur éligibilité aux prestations, ainsi que les termes et conditions spécifiques des fournisseurs de cyber-services concernés et de se tenir informés sur tout changement.

SERVICES CYBER de TIERS à prix réduit :
Personal Cyber Risk Dashboard (surveillance des vulnérabilités) ;
Password Management Application (gestion des mots de passe)

Les preneurs d'assurance qui souscrivent à une cyber-assurance auprès de Chubb, ont la possibilité d'obtenir gratuitement les cyber-services susmentionnés auprès de fournisseurs tiers spécialisés, pendant une période limitée, pour autant qu'il n'existe pas encore de relation client avec le fournisseur tiers concerné lors de la conclusion du contrat et que les autres conditions soient accomplies. Par la suite, il y a l'option de continuer à acheter les cyber-services choisis à un prix réduit. Veuillez noter que la réduction spécifique varie en fonction du produit et du service et qu'elle ne peut être appliquée que si une cyber-assurance Chubb est en vigueur. Les produits et services proposés par des fournisseurs tiers sont exclusivement soumis aux conditions contractuelles, convenues entre les preneurs d'assurance et le fournisseur tiers. La décision d'acheter un produit ou un service auprès d'un fournisseur tiers relève de la seule responsabilité du preneur d'assurance. Chubb n'assume en outre aucune responsabilité pour les produits ou services proposés par les fournisseurs tiers concernés.

Les présents contenus ont pour seul objet une information générale. Il ne s'agit pas ici de conseils personnels ni d'une recommandation destinée à des personnes privées ou à des entreprises concernant un produit ou une prestation de service. Vous trouverez les conditions exactes de couverture dans les documents d'assurance.
Chubb Assurances (Suisse) SA / Chubb Versicherungen (Schweiz) AG / Chubb Insurance (Switzerland) Limited, Bärengasse 32, 8001 Zurich, T + 41 43 456 76 00, chubb.com/ch-fr

Nous utilisons les renseignements personnels que vous nous fournissez [ou, le cas échéant, à votre courtier d'assurance] à des fins de souscription, d'administration des polices, de gestion des sinistres et d'autres fins d'assurance, comme nous l'avons décrit plus loin dans notre politique de confidentialité principale, disponible ici: https://www.chubb.com/ch-fr/footer/privacy-policy.html