Cyberattaque – Questions et réponses

Version : 28/04/2022

Des données sont-elles concernées par la cyberattaque et, le cas échéant, lesquelles ?

Selon les derniers éléments, des données ont fuité. Nous analysons actuellement l'étendue des données concernées.

D'après nos connaissances actuelles, des adresses e-mail et mots de passe de nos collaborateurs ont fuité. Nous avons pris des contre-mesures adaptées immédiatement après avoir eu connaissance de la situation et avons délivré de nouveaux mots de passe à titre préventif.

Quelle est l'étendue de cette attaque pour KSB ?

KSB a été attaquée de manière ciblée. Quelques-uns de nos serveurs et certains terminaux ont été compromis par l'attaque. Notre réaction très rapide et conséquente nous a permis d'empêcher des dommages durables.

Quel a été le processus d'analyse et quelles mesures ont été prises ?

Des anomalies ont été constatées à un stade précoce sur un serveur ; nous avons alors très rapidement décidé de déconnecter l'ensemble de l'entreprise du réseau Internet afin d'empêcher toute autre intrusion, de circonscrire les dommages et d'éviter un cryptage. Notre équipe IT travaille avec des spécialistes externes pour limiter les dommages.

Nous avons par la suite arrêté tous les systèmes afin d'effectuer une analyse correcte. Cela a eu pour conséquences la restriction de notre communication et l'interruption de notre production sur plusieurs sites pendant quelques jours. L'analyse disponible à ce jour indique que cette attaque n'a compromis que quelques-uns de nos serveurs.

La sécurité prime sur la rapidité en ce qui concerne la restauration des serveurs. Tout d'abord, les serveurs de communication et de production ont été restaurés. Il existe ensuite une priorisation interne pour les étapes suivantes. Un examen forensique est exécuté sur l'ensemble des serveurs avant leur mise en service et les serveurs sont ré-installés si nécessaire. Tous les serveurs sont en outre durcis.

Où en sommes-nous quant à l'élimination des dommages ?

Les systèmes qui avaient été compromis ont été entièrement ré-installés.

Les principaux systèmes de communication et de production ont été remis en marche au milieu de la semaine 16. Les travaux progressent rapidement et dans les délais impartis. Chaque jour, de nouveaux systèmes sont mis à disposition et opérationnels.

Nous estimons que tous les systèmes importants seront à nouveau disponibles dans le monde entier à la mi-mai.

Quelles autorités publiques ont été informées et quelle assistance ont-elles apportée ?

Nous avons immédiatement notifié l'autorité responsable de la protection des données pour le Land de la Rhénanie-Palatinat et déposé une plainte. La police et le ministère public enquêtent. Nous avons apporté notre entière assistance à ces organismes. Le ministère de l'économie de Rhénanie-Palatinat nous a en outre offert son soutien.

Les éventuelles déclarations obligatoires dans les pays hors Allemagne ont été effectuées par le biais de nos filiales respectives.

Quelles mesures sont prises pour éviter de nouvelles attaques ?

Nous faisons toute la lumière sur les faits avec des spécialistes externes. Nous utilisons les enseignements tirés de cette cyberattaque repoussée pour rendre nos systèmes informatiques encore plus résilients grâce à des mesures techniques et organisationnelles de cyberprévention et de cyberdétection.

Qu'en est-il du site web de KSB ?

Le site web www.ksb.com ainsi que les différents sites nationaux sont de nouveau en ligne. Des mises à jour quant à l'avancement des travaux y sont régulièrement publiées.

Certaines fonctionnalités, telles que le Web-Shop ou les programmes de sélection, ne sont pour le moment pas disponibles. Nous travaillons actuellement à leur remise en service.