REFERENCE CLIENT

: Groupe AFNOR

72 heures pour réagir.

AIRBUS

Aperçu

Client	Groupe AFNOR
Challenges	• Réponse à incident suite à une cyberattaque • Implémentation d'un service de supervision information (SOC)
Les solutions	• Analyse forensique et réponse à incident • SOC

Le client

Le Groupe AFNOR est une association française dont l'objectif est de concevoir des solutions basées sur les normes volontaires de confiance. Sa mission est d'accompagner les organisations et les individus dans l'application de ces normes.

La situation :

menace par rançongiciel

En février 2021, le Groupe AFNOR a été infecté par un rançongiciel. Certains de leurs fichiers ont été chiffrés et la plupart des serveurs sont devenus inaccessibles. L'infection provenait d'un email de phishing, envoyé 3 jours avant la cyberattaque.

La solution : Airbus Protect

Après l'arrêt du système d'information du Groupe AFNOR, l'Association devait comprendre précisément ce qui s'était passé, avant d'entamer **la restauration de ses systèmes**.

C'est alors qu'Airbus Protect est intervenu pour étudier les traces de l'attaque et identifier l'origine du problème. C'est la première étape pour une équipe de réponse aux incidents de sécurité informatique : **l'investigation**. En seulement trois jours, nos experts CSIRT ont pu reconstituer toute la chaîne de compromission.

Grâce à cela, il n'a fallu que **8 jours pour que le Groupe Afnor soit à nouveau opérationnel.** Au total, il aura fallu 3 mois pour reconstruire l'ensemble du système d'information. Pendant la phase de réponse, nos experts SOC ont mis en place une « supervision de circonstance » (un SOC rapidement déployable qui nous a permis d'agir rapidement pendant la crise).

Afin de s'assurer que les hackers ne puissent pas ré-exploiter les backdoors (portes dérobées), nos experts ont aidé le Groupe AFNOR à mettre à jour leurs outils et à reconstruire **l'ensemble du système d'infrastructure**. C'est ce que nous appelons la phase de « durcissement ».

Comment éviter que cela ne se reproduise ?

Après la phase de remédiation, le groupe AFNOR a souscris avec Airbus Protect à un service de supervision informatique (un SOC) par le biais du déploiement de différents outils de surveillance afin d'étendre la couverture de son système d'information et d'avoir une **nouvelle approche de détection**.

Airbus Protect a également recommandé de **sensibiliser les collaborateurs** pendant plusieurs mois, avec des campagnes de phishing et de hack de mots de passe. Cela a incité les employés du groupe AFNOR à créer des mots de passe plus forts et à avoir de meilleurs réflexes concernant les emails et les pièces jointes.

Le mot de l'expert :

"Lorsque l'on est confronté pour la première fois à ce type de crise, on est momentanément abasourdi. C'était un réel avantage de pouvoir compter sur un partenaire fiable tel qu'Airbus Protect et d'avoir à nos côtés des intervenants experts pour nous aider à gérer la crise."

Jean-Marc Aubert, RSSI du Groupe AFNOR

Réunissant une expertise exceptionnelle en matière de sûreté, de cybersécurité et de sustainability ; Airbus Protect est un leader européen en matière de gestion des risques

Nos offres de cybersécurité mentionnées dans cette référence client

SOC

Nous protégeons nos clients contre les cybermenaces connues et inconnues. Nos centres d'opérations de sécurité (SOC) offrent des services complets de bout en bout, en 24/7, à partir de locaux sécurisés situés au Royaume-Uni, en France, en Allemagne et en Espagne.

Services CSIRT

Se remettre rapidement d'un cyberincident grâce à notre équipe d'intervention en cas d'incident de sécurité informatique.

Contactez nous
protect@airbus.com

Découvrez d’autres case studies sur notre site web

www.protect.airbus.com

AIRBUS

Airbus Protect, 31700 Blagnac, France