N°6596
Entrée le 16.08.2022

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Énergie et de
l'Aménagement du territoire

Département de l'énergie

Äntwert vum Minister fir Energie op d'parlamentaresch Fro n°6596 vum 2. August 2022 vum éierewäerten Deputéierte Sven Clement iwwert eng Cyberattack op Creos

1. Si bei dëser Attack effektiv perséinlech Informatioune vun den Hacker geklaut ginn? Waren hei och Kontonummeren dobäi?

Op Nofro hin huet Encevo informéiert, dass d'Analyse vun den Donnéeën, déi geklaut goufen nach am gaangen ass. Dem aktuelle Wëssensstand no sinn ënnert de geklauten Informatiounen och allgemeng Basisdonnéë wéi Nimm, Virnimm, Adressen an, falls gespäichert, E-Mail-Adressen an Telefonsnummere souwéi Bankverbindunge vu bestëmmte Clientsgruppen.

2. Wa jo, ass dem Ministère bekannt, ob dës Date veröffentlecht goufen?

Dem Ministère, souwéi Encevo, ass bekannt, dass et zanter der Attack effektiv eng Veröffentlechung vu geklauten Informatiounen am sougenannten Darknet ginn ass. Déi Situatioun gëtt och weiderhin an Zesummenaarbecht mat de responsabelen Autoritéite genau iwwerwaacht.

3. Ass d'CNPD iwwert dës Cyberattack informéiert ginn? Wa nee firwat net?

Soubal d'Attack bemierkt ginn ass, huet Encevo nieft der Bekämpfung vun der Attack och all aner néideg Mesure geholl, dat heescht ënner anerem sinn och déi jeeweileg Autoritéiten (Police, GovCert, ILR…) informéiert ginn. Dozou gehéiert och eng Notifikatioun un d'CNPD. Bei all dësen Notifikatioune sinn déi virgeschriwwen Delaien agehale ginn.

4. Sinn d'Clientë vu Creos iwwert dës Attack, respektiv iwwert d'Fuite vun hiren Date vu Creos informéiert ginn sou wéi den RGPD dat firgesait? Wa nee firwat net?

Alleguerten d'Clientë sinn iwwer eng Kommunikatioun un de *Grand public* informéiert ginn. De Grupp Encevo, zu dem Creos gehéiert, huet méindes de 25. Juli en éischte Pressecommuniqué zu der Cyberattack gemaach an och iwwert seng jeeweileg Clients-Portaler informéiert.

En zweete Pressecommuniqué mat Hiweis op den *Data Breach* gouf dann den 28. Juli gemaach. Gläichzäiteg goufen all aner Partner a Fournisseure vu Creos respektiv Enovos iwwer Email op de potentiellen *Data breach* higewisen. Zum selwechte Moment huet de Grupp Encevo eng speziell ëffentlech Websäit opgemaach mat engem FAQ zu der Attack an dem *Data Breach*. Des Kommunikatioun gouf breet gemaach, en Fonction vun der Entwécklung vun der Situatioun a vun dem wat sécher konnt affirméiert ginn. Ee weideren drëtte Pressecommuniqué ass de 4. August gemaach ginn. Och soss gouf a Kommunikatioune mat Clienten op d'Cyberattack higewisen insofern verschidde Servicer impaktéiert waren an net wéi gewinnt konnte funktionéieren.

D'Enquête ass nach net ofgeschloss, sou dass nach net Detailer all bekannt sinn, déi et erméigleche jidder potentiell betraffe Persoun perséinlech ze informéieren. Persoune vun deene gewosst ass, dass hir persounebezunnen Donnéeë betraff sinn, ginn am Laf vun der Zäit individuell benoriichtegt.

5. Wéi ass dës Cyberattack zu stane komm a goufen dës Schwaachpunkte mëttlerweil besäitegt?

Op Nofro hin huet Encevo informéiert, dass den informatesche System vun hirem Grupp duerch fortschrëttlech Sécherheetssystemer a –Prozesser geschützt ass, déi duerch ee ronderëm d'Auer besate Sécherheetsbetribszentrum an engem IT-Noutfallteam ergänzt sinn. Des Moossnamen hätten et erméiglecht schnell ze reagéieren. Encevo investéiert bestänneg an hir Schutzmoossnamen, fir ob déi sech schnell verännerend Cybermenace reagéieren ze kënnen an d'Bestëmmungen iwwer GDPR – also déi allgemeng Dateschutzbestëmmungen – an den NIS-Reegelen – also d'Reegelen iwwer d'Sécherheet vun Informatiounssystemer – anzehalen.

D'Attack, där Encevo ausgesat war, huet eng speziell entwéckelt sophistiquéiert Schuedsoftware benotzt, déi net duerch konventionell Antivirus-Software konnt identifizéiert ginn. Souwäit méiglech huet Encevo an der Tëschenzäit d'Iwwerwaachung vun hiren Informatiounssystemer weider verstäerkt, d'Systemer opgrond vu séchere Backupen erëm eropgefuer, d'Sécherheet vum *Accès à distance* op d'Plattforme verstäerkt an alleguerten d'Passwierder geännert.

6. Wéi eng Moossname ginn en place gesat, datt déi betraffe Cliente keng negativ Konsequenzen dovunner hunn (Identitéitsklau, onerlaabte Bankofbuchungen,...)?

D'Schwaachpunkte si mëttlerweil behuewen an et ass séchergestallt ginn, dass sech keng Bedroung méi an de Systemer verstoppt. Iwwer en FAQ, den en Fonction vun der Entwécklung ausgebaut gëtt, informéiert de Grupp Encevo e.a. iwwer Risiken, méiglech Konsequenzen a gëtt Rotschléi fir Dateklau ze vermeiden. Dozou gehéiert ënner anerem d'Opfuederung fir déi bestoend Passwierder ze änneren.

Lëtzebuerg, de 16. August 2022
(s.) Claude Turmes
De Ministre de l'Énergie