N° 5604
Reçue le 01.03.2022

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de l'Économie

Réponse commune de Monsieur le ministre de l'Économie, Franz Fayot, de Monsieur le Premier ministre, ministre d'État, Xavier Bettel, de Madame la ministre de la Justice, Sam Tanson et de Monsieur le ministre de la Sécurité intérieure, Henri Kox, à la question parlementaire n° 5604 du 28 janvier 2022, de Monsieur le député Sven Clement, concernant les attaques informatiques de type « phishing »

1.

Déi 3 lescht Joer goufe folgend Unzuele vu Plainte wéinst Phishing Attacke gemaach:
2019 : 5
2020 : 26
2021 : 41

De Service de Police Judiciaire ass vum Parquet mat folgenden Unzuele vun Enquête chargéiert ginn:
2019 : 4
2020 : 7
2021 : 0

Beim GOVCERT, also dem CSIRT (Computer Security Incident Response Team) vun der Lëtzebuerger Regierung goufe folgend Unzuele vu Phishing E-Maile an de leschte Jore behandelt:
2019 : 1.265
2020 : 3.214
2021 : 5.157

Beim CIRCL, dem CERT (Computer Emergency Response Team) fir den Privatsecteur, d'Gemengen an d'net-Regierungs Organisatiounen zu Lëtzebuerg, si folgend Unzuele vu Meldunge vu Phishing erakomm:
2019 : 1.304
2020 : 1.589
2021 : 1.080

2.

Den monetäre Schued vun dësen Attacken ass schwéier ze chiffréieren an et ass net méiglech heizou zouverléisseg Chifferen ze nennen.

Direkt Käschten am Sënn vu Bezuele vun Erpressungsgelder oder opgrond vu Strofen duerch Verletzunge vun der GDPR, als Suite vun enger Phishing Attack, déi beim Staat ugefall wiere goufen dem GOVCERT keng gemellt.

3.

An deene leschten 3 Joer, goufe wéi ënnert dem Punkt 1) opgelëscht 72 Plainte deposéiert. Vun deenen 72 Plainte goufen der 7 vu Firmen deposéiert an 65 vu Privatpersounen.

4.

An 10 vun den Affären déi ënnert dem Punkt 3) detaillléiert goufe gëtt momentan nach ermëttelt. 62 Affäre si klasséiert gi well den Täter net konnt ermëttelt ginn. D'Opklärungsquote bei Phishing ass also relativ geréng, 2021 konnten awer an enger internationaler Operatioun an Zesummenaarbecht mat Europol a Rumänien dräi Täter verhaft ginn, déi och fir Phishing zu Lëtzebuerg verantwortlech waren.

5.

D'Utilisateure gi reegelméisseg a weiderhi vum CIRCL an vum GOVCERT iwwer d'Gefore vu Phishing E-maile sensibiliséiert, a ginn forméiert fir net all Link an all E-mail unzeklicken ouni sech ze froen op den E-mail authentesch a plausibel ass.

Wann een Mataarbechter vu Staat generell Zweiwel huet op een E-mail authentesch (oder infizéiert) ass, kann déi betraffe Persoun den E-mail ganz einfach, mat engem Klick, duerch dem GOVCERT säi Service „GC NOTIFY" („Report Mail" Funktioun an der E-mail Applikatioun vum Staat) analyséiere loossen. An Zukunft gëtt dëse Service nach méi promovéiert. An dësem Sënn huet de GOVCERT d'lescht Joer sophistiquéiert Anti-Phishing Campagnë bei verschiddenen Administratioune gemaach. Hei goufe Phishing Attacke simuléiert an da gemooss wéi vill Prozent vun den Agenten op een (simuléierten) Phishing E-mail erafalen, an ergo nach net genuch sensibiliséiert sinn. Dono huet de GOVCERT déi betraffe Persoune kontaktéiert an erkläert wat si an Zukunft besser kënne maachen.

Op der Säit vun der Infrastruktur, vir den Impakt vu Phishing Campagnen ze limitéieren, instruéiert de GOVCERT de CTIE, déi staatlech Cyber Defense Systemer esou ze konfiguréieren, a gefälschten E-mailen esou ze traitéieren, datt et an der Folleg net zu enger Infektioun vu staatlechen IT-Systemer kënnt, wat jo oft dat eigentlecht Ziel vun enger Phishing Attack ass.

Wann de GOVCERT gesäit datt déi national Telekommunikatiounsentreprise betraff sinn, oder si an hirem Rôle als Operateur eppes géint déi spezifesch Phishing Attack kënnen ënnerhuelen, kontaktéiert de GOVCERT des Operateuren entspriechend de Prozeduren déi festgehale sinn.

De CIRCL op senger Säit kommunizéiert iwwert automatiséiert Kanäl mat de groussen nationalen an auslänneschen Operateure fir se iwwert d'Usurpatioun vun Domän-Nimm ze informéieren op déi d'Utilisateuren dirigéiert ginn. D'Zil ass hei déi béisaarteg Websäiten ze stoppen ier en Affer vum Phishing seng Benotzer-Daten an säi Passwuert konnt aginn. Déi vu Phishing-Campagne betraffe Servicer (Banken, Luxtrust...) ginn ëmmer schnellstméiglech informéiert.

6.

Am Kader vun den Ermëttlungen an de Fäll vu Phishing gëtt esouwuel um europäeschen ewéi och um internationalen Niveau déi traditionell „coopération judiciaire" benotzt. Phishing fält des weideren ënnert déi allgemeng international Kooperatioune vun der Police am Beräich Cybercrime.

De CIRCL tauscht och international mat Partneren Informatiounen aus fir dass Phishing-Aktiounen déi rapportéiert gi sinn och kennen a Lëschte vu blockéierten Internetsäite vun de Browseren opgeholl ginn, sou dass eventuell Affer vum Phishing net méi op dës béisaarteg Säite kenne goen.

Lëtzebuerg ass och am Reseau vun de weltwäite CERTen gutt connectéiert. De GOVCERT an de CIRCL sinn um internationalen Niveau a verschiddene Gremien an Organisatiounen aktiv, wou d'Experte kucke wéi eng Mechanisme kënnen agesat gi fir datt mir um internationalen Niveau eng E-mail Infrastruktur kréien, déi et erlaabt d'Problematik vu Phishing E-maile besser unzegoen an esou den Utilisateur besser ze schützen.

Am konkreetste sinn do d'Initiativen um Niveau vun der EU, méi spezifesch d'Initiative „Modern Email Security Standards for EU (MESSEU)", déi aktiv den DKIM ("DomainKeys Identified Mail") Standard an den DMARC ("Domain-based Message Authentication, Reporting & Conformance") Protokoll promovéiert.

D'Mise en Place vun dëse Mesuren awer ass eng komplex an technesch Matière. Staark vereinfacht ausgedréckt, leeft et dorobber eraus datt all E-mail Serveur an E-mail Utilisateur muss authentifizéiert ginn, an dann nëmmen nach E-Mailen ugeholl ginn, wou et vun der Infrastruktur hir bekannt ass datt den E-mail vun engem authenteschen E-mail Serveur/Utilisateur kënnt. Dat ass schonn eng immens Verbesserung zu den aktuellen E-Mail-Protokollen, mee wäert awer trotzdeem net all Phishing Attacke kënnen ënnerbannen. An et wäert och nach dauere bis international eng kritesch Mass un E-mail-Service Bedreiwer deem konform wäert sinn; eng kritesch Mass gëtt awer gebraucht fir Phishing Attacke kënnen effizient ze bekämpfen.

De GOVCERT an de CTIE sinn zesummen, am Kader vun der Ëmsetzung vun der SNCS (Strategie nationale en matière de cybersecurité), drun ze evaluéieren ënnert wéi enge Contrainten DKIM an DMARC op der staatlecher Säit kënnen implementéiert ginn, fir an Zukunft zumindest beim Staat ee bessere Schutz géint dës Phishing Attacken ze hunn.

Um Terrain ass de GOVCERT am direkten Echange mat anere Länner, wéi zum Beispill mat den Homologe vum NUKIB an Tschechien.

Luxembourg, le 1. mars 2022

Le Ministre de l'Économie

(s.) Franz Fayot