carte usage numérique

cyber malveillance.gouv -> recommandation

Victime

Modalité

Compte rendu du changement ( comment faire appliquer une charte d’usage numérique cyber pour protéger une organisation )

src: <https://www.latribune.fr/economie/international/la-coree-du-nord-accusee-du-piratage-de-la-banque-centrale-du-bangladesh-669215.html>

<https://www.lefigaro.fr/flash-eco/2015/02/16/97002-20150216FILWWW00058-une-gigantesque-cyber-fraude-decouverte.php>

https://www.linkedin.com/pulse/case-study-bangladesh-banking-heist-digialert

Le site web officiel et les communications de la Society for Worldwide Interbank Financial Telecommunication (SWIFT), en particulier après 2016.

Les rapports des entreprises de cybersécurité telles que BAE Systems, Symantec et FireEye, qui ont fourni des analyses détaillées des logiciels malveillants utilisés dans l'attaque.

Les déclarations officielles et les inculpations du département de la Justice des États-Unis liées à l'affaire.

Malheureusement, en raison des limitations de mon interface, je ne peux pas fournir de liens directs. Cependant, les sources mentionnées devraient être facilement accessibles via les moteurs de recherche ou les sites web officiels respectifs.

https://www.bbc.com/afrique/monde-57573326



Sujet: Banque centrale du Bangladesh

Contexte: Détournement de fond ( vise 1 milliard, 81 millions de dollars au final )

1. Aperçu :

En février 2016, des cybercriminels ont tenté de voler environ 1 milliard de dollars du compte de la Bangladesh Bank à la Federal Reserve Bank de New York. Ils l'avaient fait en initiant des demandes de transfert via le réseau SWIFT, utilisé par les banques du monde entier pour autoriser les transferts interbancaires.

2. Méthode d'attaque :

Bien que la méthode exacte par laquelle les assaillants ont eu accès aux systèmes de la Bangladesh Bank demeure en partie spéculative, on pense qu'ils ont exploité les vulnérabilités des systèmes internes de la banque et ont peut-être obtenu un accès initial via un courriel d'hameçonnage.

Une fois à l'intérieur, ils ont compromis l'interface logicielle SWIFT appelée Alliance Access et l'ont utilisée pour envoyer de multiples ordres de transfert de grande valeur.

3. Les transferts :

Sur les 35 demandes effectuées par les pirates, la majorité a été signalée pour examen manuel ou bloquée en raison d'irrégularités. Cependant, cinq de ces demandes, totalisant 101 millions de dollars, ont abouti. Sur cette somme, 20 millions de dollars envoyés à une banque sri-lankaise ont été récupérés grâce à une simple erreur typographique commise par les pirates, rendant le transfert suspect. Mais les 81 millions de dollars restants envoyés aux Philippines ont disparu et ont été retracés jusqu'aux casinos et aux opérateurs de junket.

4. Conséquences :

Le vol a soulevé d'importantes questions concernant la sécurité du système SWIFT. En réponse, SWIFT a reconnu que l'incident de la Bangladesh Bank n'était pas un cas isolé et que d'autres banques avaient été ciblées de manière similaire. Par conséquent, SWIFT a introduit des mesures de sécurité supplémentaires et a exhorté les banques membres à renforcer leurs précautions en matière de sécurité.

L'incident a également entraîné d'importantes modifications au sein de la Bangladesh Bank, notamment la démission de son gouverneur, Atiur Rahman.

5. Enquête :

Les rapports d'experts en criminalistique ont suggéré que le groupe Lazarus, lié à la Corée du Nord, était derrière l'attaque. Le département de la Justice des États-Unis, en 2018, a inculpé un individu nord-coréen nommé Park Jin Hyok pour sa participation au vol et à d'autres cyberattaques.

6. Leçons :

Le vol a souligné l'importance de la cybersécurité dans le secteur financier et a mis en lumière la nécessité de protocoles de sécurité stricts. Il a montré que même les réseaux les plus sécurisés, comme SWIFT, peuvent être vulnérables si la sécurité des points d'extrémité dans les banques individuelles est compromise.

7. Solutions :

* Former régulièrement les employés aux dernières menaces

- Réaliser des audits de sécurité réguliers pour identifier et corriger les vulnérabilités.

* Utiliser l'authentification à deux facteurs ou multi-facteurs pour accéder aux systèmes sensibles.