La Banque Centrale Tunisienne Victime d'une cyberattaque

Mzoughi Mohamed Amine

Septembre-novembre 2022

Professeurs : Touba Keltoum, Louadj Kamila.

Etablissement/Formation : IUT Villetaneuse – BUT Réseaux et Télécommunication.

Table des matières :

Introduction :

Les cyberattaques ont augmenté de 50% depuis le début de la pandémie (covid-19) ce qui engendre beaucoup de perte financière soit au niveau de l'entreprise ou au niveau du pays surtout qu'en ce moment, les guerres sont devenues informationnelle et non plus physiques (infoguerre). C'est pour cela que j'ai choisis de parler, aujourd'hui, d'une cyberattaque qui a visé la Banque Centrale de la Tunisie, le 23 mars 2022, et dans laquelle des criminels ont utilisés la méthode de phishing dans le but de récolter des informations personnelles. La question qui se pose est la suivante : En quoi une attaque informatique peut menacer la sécurité de tout un pays ? Pour répondre à cela, on va définir tout d'abord l'entreprise, puis on va voir les enjeux et détails de cette attaque informatique, et pour finir, on verra les effets post-attaque qui vont répondre à notre question.

I/ Présentation de la banque centrale tunisienne.

1)Présentation générale.

La Banque centrale de Tunisie (BCT) est la banque centrale tunisienne, son siège est à Tunis et son gouverneur est l'économiste tunisien Marouane Abassi depuis le 16 février 2018.

Elle représente un établissement économique public et est doté de personnalité morale et de l'autonomie financière. La BCT est indépendante dans la réalisation de ses objectifs, l'exercice de ses missions et la gestion de ses ressources. Elle est soumise au suivi de l'assemblé des représentants du peuple.

Et on note bien que les personnels de la BCT sont soumis à un statut particulier approuvé par décret gouvernemental vu l'importance et la sensibilité de leurs postes.

2)Historique.

La banque centrale de la Tunisie a été fondée deux ans après l'indépendance du pays (le 19 septembre 1958).

Voici une liste des événements les plus importants dans l'historique de la BCT :

Le 20 mars 1956 : Indépendance de la Tunisie.

Le 19 septembre 1958 : Promulgation de la loi n°58-90 portant création et organisation de la Banque Centrale de Tunisie.
Le 18 octobre 1958 : Promulgation de la loi n°58-109 portant réforme monétaire. Institution d'une nouvelle unité monétaire : le Dinar.
Le 3 novembre 1958 : Entrée en activité de la Banque Centrale de Tunisie et mise en circulation du Dinar tunisien.
Le 30 décembre 1958 : Décrochage du dinar du franc français et sortie de la monnaie nationale de la zone franc.
Le 7 décembre 1967 : Promulgation de la loi n°67-51 portant réglementation de la profession bancaire.

3 novembre 1988 :Réforme globale des textes organiques de la BCT, loi n°1988-119 du 3 novembre 1988:

* Remplacer les fonctions des deux sous gouverneurs et du secrétaire général par celle d'un vice-gouverneur chargé d'assister le gouverneur ;
* Préciser davantage le rôle de la BCT en vue de défendre la valeur de la monnaie nationale et de veiller à sa stabilité;
* Interdir à la BCT de participer au capital d'entreprises résidentes et transférer au profit de l'Etat toutes ses participations dans ces entreprises.

7 février1994 : Modification de la législation régissant la profession bancaire apportée par la loi n° 94-25 du 7 février 1994 renforçant les pouvoirs de réglementation et de surveillance conférée à la Banque Centrale de Tunisie.

On peut dire aussi que depuis l'intégration d'un service informatique dans la banque centrale de la Tunisie en 2004 ils ont connu bien sur quelques problèmes technique et faille informatiques mais qui n'ont pas eu de conséquence graves sur le fonctionnement de la banque. Par exemple les arrêts du site officiel ou pertes de données...

3)Missions et rôles sensibles.

Pour commencer, on doit préciser qu'il n'existe pas un seul type de banques centrales, car chaque pays peut lui accorder des missions, et lui conférer des outils, différents. Les lois nationales ou des traités supranationaux peuvent également contraindre la banque centrale ou lui donner des pouvoirs d'action supplémentaires.

On peut citer les principaux rôles de la BCT :

-Assurer la stabilité monétaire, en effet, La plupart des banques centrales a pour mission d'assurer la stabilité monétaire, c'est-à-dire la stabilité des prix. Elle doit dans ce cas veiller à ce que l'inflation(1) ne dépasse par une borne fixée à l'avance.

-La supervision financière : La banque centrale peut aussi disposer d'un rôle de supervision et de régulation du fonctionnement des marchés financiers. Elle doit ainsi assurer le respect des réglementations du risque (ratio de solvabilité(2)) des institutions financières(3), et en particulier des banques de dépôts).

-Fixation des taux directeurs : La banque centrale a un pouvoir important car elle dispose de leviers d'action que sont les taux directeurs(4). Ces taux, appliqués aux banques de second rang(5), permettent de moduler les coûts de financement et de refinancement des banques, **et influe ainsi sur l'activité économique.**

La BCT aussi peut jouer le rôle d'un préteur pour les banques économiques tels que : Zitouna Bank, Attijari Bank...

PRESENTATION DU SYSTEME FINANCIER TUNISIEN

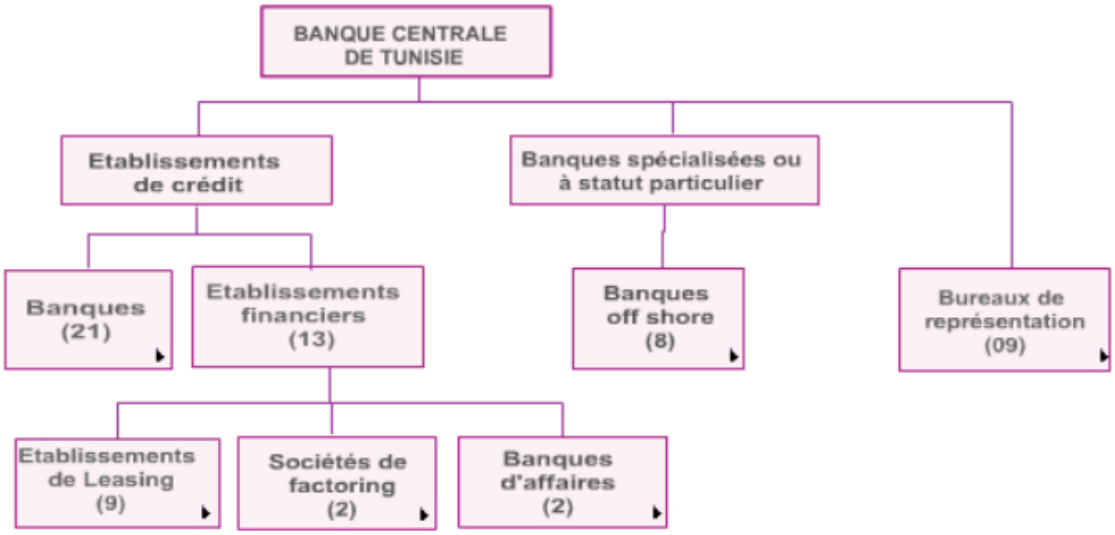

Figure (1)

Donc on peut constater que la BCT représente le moteur de l'économie du pays et a un rôle très essentiel dans la stabilité et la sécurité du pays. Vu l'importance et la place de la BCT dans le pays, cette dernière peut être une cible pour des attaques informatiques, et c'est ce qu'on va voir dans la 2éme partie.

II/ Détails et enjeux de la cyberattaque.

Dans un communiqué de presse, le dispositif de sécurité informatique de la Banque centrale de Tunisie annonce avoir détecté, dans la matinée du

Mercredi 23 mars 2022, une attaque cybernétique.

1) Identification des attaquant (hackers)

Malgré le développement des outils de sécurité, il demeure très rare d'identifier les hackers dans une cyberattaque.

Ces derniers utilisent des méthodes très avancé dans le but de rester anonyme et ne pas dévoiler leurs informations personnelles tels que leurs nationalités (qui peut poser problème dans les relations internationales entre les pays).

Même si des fois on trouve des pistes qui vont nous permettre d'identifier le hacker, elles sont, la plupart du temps, fausses vu qu'un attaquant utilise des identifiants qui soit n'existe pas ou qui appartiennent à quelqu'un d'autre (Utilisation d'autre VPN(6) par exemple).

La BCT a pourtant chargé l'ANSI(7) de mener une enquête dans le but d'identifier les attaquants.

2) La méthode utilisé (explication de la méthode de fishing).

Le 23 mars 2022, une page Facebook est apparue avec un nombre d'abonnements énormes et qui se prend pour la page officielle de la Banque centrale de la Tunisie. Cette page a communiqué à ces abonnés un lien web dans lequel on leur demande de mettre à jour leurs informations personnelles tel que leurs adresses postales, informations bancaire (RIB, code du compte...).

Ce site avait l'air très crédible vu qu'il a été publié sur une grande page Facebook.

Ainsi, le fait de mettre en pression l'utilisateurs (par exemple dans notre cas, si l'utilisateurs ne mets pas à jour ces informations personnelles, son compte bancaire pourrait se bloquer) sert comme outil pour le convaincre.

Heureusement, cette attaque a été contrôlé grâce au blocage de la page ainsi que le site crée.

On appelle cette méthode de piratage le Phishing :

L'hameçonnage ou phishing est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, numéro ou photocopie de la carte d'identité, date de naissance, etc. En effet, le plus souvent, une copie exacte d'un site internet est réalisée dans l'optique de faire croire à la victime qu'elle se trouve sur le site internet officiel où elle pensait se connecter. La victime va ainsi saisir ses codes personnels qui seront récupérés par celui qui a créé le faux site, il aura ainsi accès aux données personnelles de la victime et pourra dérober tout ce que la victime possède sur ce site. L'attaque peut aussi être réalisée par courrier électronique ou autres moyens électroniques. Lorsque cette technique utilise les SMS pour obtenir des renseignements personnels, elle s'appelle SMiShing.

-Pour en savoir plus sur le Phishing, je vous mets dans l'annexe le lien d'une vidéo sur YouTube, que j'ai réalisé l'année dernières avec mon collègue. Cette dernière explique <u>en anglais</u> la méthode de phishing et comment se protéger de ce type d'attaques informatiques.

3) Les cibles de cette attaque.

La méthode de phishing (ou hameçonnage) peut viser, comme le reste des attaques cybernétiques, les personnels de l'entreprise et surtout le service informatique vu que ces derniers ont accès aux informations secrètes de l'entreprise. Mais dans notre cas, les utilisateurs de la BCT sont les cibles de l'attaque.

Cela pose moins de risque pour l'entreprise vu que le service informatique ne serait pas directement touché et donc l'intervention serait moins compliquée et plus rapide.

Donc on ne peut pas vraiment parler de faille dans le système informatique de l'entreprise.

Même si cette attaque a été maitrisée, cette dernière a engendré des effets, c'est ce qu'on va voir dans la prochaine partie.

III/ Le Post-attaque.

1) Les dégâts au niveau de l'entreprise.

Qu'elles soient directes ou indirectes, les pertes liées à la cybercriminalité demeurent significatives. Les banques étant soumises à des exigences réglementaires strictes ont un coût moyen de violation de données nettement supérieur à celui des entreprises moins réglementées comme l'hôtellerie, les médias et la recherche.

Heureusement, vu que ce phishing a visé des utilisateurs et non pas le service informatique, cette attaque n'a pas eu des effets néfastes sur La Banque Centrale Tunisienne.

Des perturbations sur certaines de ces activités ont été enregistré entre le 23 et le 24 mars 2022. On peut par exemple citer les services en relation avec le système bancaire tel que le retrait, le dépôt d'argent...

Cela a causer des pertes économiques pour l'entreprise qui a eu un ralentissement dans 30% de ses activités.

On rappelle aussi que la réputation de l'entreprise est touchée à chaque fois qu'elle soit ciblée par une cyberattaque. Ce qui fait que le client ne se sent plus en sécurité.

En terme général, dans le secteur financier, une étude américaine publiée en 2018 par Bouveret estime que « **la perte moyenne annuelle liée aux cyberattaques représenterait environ 10 % du résultat net des banques au niveau mondial, soit environ 100 milliards de dollars** ».

Vu l'importance de la BCT et la sensibilité de son rôle dans l'économie tunisienne, cette attaque a eu aussi un effet sur le pays.

2) Les effets sur le pays.

La Banque Centrale de la Tunisie représente l'unité centrale de l'économie du pays, donc le moindre problème qu'elle rencontre, peut décélerer l'activité du pays ainsi que le fonctionnement du reste des banques économiques.

Le ralentissement des activités bancaires engendre le ralentissement du reste des activités économiques (import, export, bourse, achat-vente...).

Après 10 jours de cette cyberattaque, le dinar tunisien a chuté de 0.0001% de sa valeur.

Cette attaque n'a pas seulement le but de voler de l'argent, mais aussi de menacer la sécurité du pays vu qu'on vise une entreprise publique et non pas prive. Le président de république Tunisien Kais Saied a reçu le 24 mars 2022 le ministre des Technologies de l'information et de la communication pour insister sur la nécessité de prendre toutes les mesures en prévention des cyberattaques.

Cette cyberattaque a poussé donc les responsables informatiques de prendre des mesures et des précautions afin d'éviter, le plus que possible, d'autres attaques.

3) Des nouvelles mesures et précaution.

Pour mieux se protéger contre les cybercriminalités, les services informatiques mettent à jours leurs outils, stratégies de défenses...

La BCT a commencé par des travaux sur son site internet, ils ont amélioré les services que propose le site ainsi que la partie backend(1) pour augmenter la sécurité d'accès. Ces travaux ont duré 24 heures ce qui a aussi ralentit le fonctionnement de la BCT.

Le ministère des Technologies de la communication a mis en œuvre une compagne dans le but de rappeler aux différentes institutions publiques et privées à mettre en œuvre les mesures de sécurité de l'information nécessaires, à relever le niveau de vigilance, à mettre à jour les plans de continuité d'activité et à s'assurer de leur efficacité et de leur capacité à assurer la continuité des missions en cas de cyber-accidents. Elle a également souligné que l'Agence nationale de sécurité informatique (ANSI) met à la disposition des établissements toutes les mesures techniques nécessaires pour protéger les réseaux et les systèmes d'information des dangers de propagation des rançongiciels pendant cette période.

Mise en place d'un numéro vert pour les victimes de cyberattaques dans le but de les guider à faire les bonnes pratiques.

Augmentation de budget accordé à la cyberdéfense au sein du service informatique de la BCT.

Ainsi, vu que les cyberattaques sont définies comme des criminalité, le Parquet du Pôle Judiciaire Antiterroriste a engagé une enquête.

Le premier juge d'instruction du Pôle judiciaire antiterroriste en a été chargé, annonce un communiqué, rendu public le lundi 11 avril 2022, par le Bureau de l'information du Tribunal de première instance de Tunis, qui précise, également, que les investigations sont toujours en cours.

L'article 323-1 du code pénal sanctionne « le fait d'accéder ou de se maintenir frauduleusement, dans tout ou partie d'un système de traitement automatisé ». La peine encourue est **2 ans d'emprisonnement et à l'équivalent de 30000€ d'amende**.

L'ANSI a aussi rappelé que d'après l'article 2 du décret n° 2013-4506 du 6 novembre 2013, relatif à la création de l'agence technique des télécommunications énonce notamment que : « L'agence technique des télécommunications assure l'appui technique aux investigations judiciaires dans les crimes des systèmes d'information et de la communication, elle est à cet effet chargée des missions suivantes: [1] la réception et le traitement des ordres d'investigation et de constatation des crimes des systèmes d'information et de la communication issus du pouvoir judiciaire conformément à la législation en vigueur ; [...] [2] l'exploitation des systèmes nationaux de contrôle du trafic des télécommunications dans le cadre du respect des traités internationales relatifs aux droits de l'Homme et des cadres législatifs relatifs à la protection des données personnelles ».

Mes propositions :

-Mise en œuvre d'un système d'exploitation plus développer et sécurisé (Linux ou dernières versions de Windows), à noter qu'une partie du système informatique de la BCT utilise toujours Windows 7.

-Création de réseaux sociaux (Facebook, Instagram...) certifiés identiques.

Conclusion :

Cette cyberattaque est une parmi beaucoup d'autres attaques que subissent toutes les entreprises de différentes activités et partout dans le monde et qui par le biais d'un piratage de quelques ordinateurs, peuvent toucher l'économie de tout un pays et donc de menacer sa sécurité. Pour cela, il reste très important de mettre en œuvre des protocoles et stratégies de sécurité afin de diminuer leurs effets. Cela m'apprend à mieux gérer mes données (surtout les mails ou SMS de phishing que je reçois tous les jours).

La nouvelle technologie facilite nos vies mais l'un des défauts les plus pertinents est la protection et la sécurité de ces derniers. Est-ce qu'on pourrait un jour avoir des systèmes informatiques sécurisés à 100% ?

Abstract:

Today, the world is more digitally connected than ever before. Criminals take advantage of this online transformation to target weaknesses in online systems, networks and infrastructure. And today we are taking the example of a cyber-attack that targeted the Central Bank of Tunisia which took place on March 23, 2022.

To start, the Central Bank of Tunisia (BCT) is a public establishment created on the 19th of September 1958 (2 years after the independence), it has several sensitive missions and roles that directly affect the country's economy (like financial stability, loans, stock exchange...).Given the importance of this company, it remains a good target for Internet criminals.

By using phishing method (wich is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message), ananymous atackers took themselves for BCT personnals by creating a Facebook. This page shares a fake link wich asks BCT users (or clients) to update their personal informations

(Payement and banking informations, address...). Fortunately, the BCT have announced the total control of this attack thanks to ANSI group who has blocked the fake Facebook page and the Website. Even if this attack was mastered, it had some side effects. The company had a slowdown in its economic activities and banking services. This fact caused an economic incident throughout the country (in view of the sensitive role of the bank). As we know, every economic problem may cause social issues which threatens the country's safety. Even the president of the republic (Kais Said) intervened to report it as a terrorist attack who aims to destabilize internal security. This attack prompted officials to implement new security measures to enable better data protection(website update, cybersecurity awareness...).

We can say that, even when the BCT have a good defense strategy, she still remains a target of cyber-attacks, that's why we need an up-to-date security systems.

Lexique :

(1): Accroissement excessif des instruments de paiement (billets de banque, capitaux) entraînant une hausse des prix et une dépréciation de la monnaie

(2):En comptabilité, un ratio est un coefficient ou un pourcentage généralement calculé entre deux masses fonctionnelles du bilan ou du compte de résultat. Les ratios servent à mesurer la rentabilité, la structure des coûts, la productivité, la solvabilité, la liquidité, l'équilibre financier, etc.

(3): En économie, une institution financière est une institution publique ou privée, qui assure une mission économique ou financière et qui fournit des services financiers à ses clients.

(4): Les taux directeurs sont les taux d'intérêt au jour le jour fixés par la banque centrale d'un pays ou d'une union monétaire, et qui permettent à celle-ci de réguler l'activité économique.

(5): Une banque de second rang (ou économique) est une institution financière qui fournit des services bancaires, soit notamment de dépôt, de crédit et paiement. Le terme de banque peut désigner de façon générale le secteur bancaire.

(6) Un VPN (Virtual Private Network) **est un « réseau privé virtuel », à savoir un service qui établit une connexion chiffrée et sécurisée entre votre ordinateur et Internet**. Ce faisant, vous bénéficiez d'un tunnel privé pour vos données et vos communications lorsque vous surfez sur des réseaux publics.

(7) L'Agence nationale de la sécurité informatique est une agence tunisienne crée en 1999 spécialisée dans la sécurité informatique.

Table des illustrations :

Annexes :

Lien vers la vidéo que j'ai réalisé en anglais et qui explique la méthode de phishing et comment se protéger face à ce type d'attaque :

Fake President Fraud -- Mzoughi Guyon

Bibliographie :

Site officiel de Mosaique FM :

https://www.mosaiquefm.net/fr/actualite-national-tunisie/1030454/la-bct-maitrise-une-attaque-cybernetique

Wikipedia:

https://fr.wikipedia.org/wiki/Banque_centrale_de_Tunisie

Site officiel de la BCT :

https://www.bct.gov.tn/bct/siteprod/actualites.jsp?id=935#:~:text=Le%20dispositif%20de%20s%C3%A9curit%C3%A9%20informatique,la%20S%C3%A9curit%C3%A9%20Informatique%20(ANSI).

AA info :

https://www.aa.com.tr/fr/afrique/tunisie-la-bct-revient-sur-la-cyberattaque-dont-elle-a-%C3%A9t%C3%A9-la-cible-/2550555

Nessma.TV

https://www.nessma.tv/fr/nationale/actu/cyberattaques-la-bct-appelle-les-banques-les-etablissements-de-credits-et-les-gestionnaires-des-infrastructures-de-paiement-et-de-reglement-a-elever-le-niveau-de-vigilance/284543

Lapresse.tn

https://lapresse.tn/126461/banque-centrale-de-tunisie-une-cyberattaque-maitrisee/

BusinessNews

...