Matinales du Groupe Le Matin en partenariat avec Dell Technologies

Cybercriminalité : Pourquoi les entreprises sont plus vulnérables

La crise sanitaire a accéléré la digitalisation des services publics et des entreprises. Cette transition qui s'opère rapidement n'est pas exempte de risques, notamment ceux liés à la cybercriminalité. Le Maroc, à l'instar d'autres pays, fait quotidiennement face à des millions d'attaques. Les plus sophistiquées d'entre elles, à peu près une dizaine, ciblent pratiquement tous les secteurs d'activité, en plus des systèmes d'information de l'État. Face à ces offensives numériques, la Direction générale de la sécurité des systèmes d'information rattachée à l'Administration de la défense nationale déploie son artillerie lourde afin de les dissuader. Mais si l'Administration publique semble immunisée, les entreprises le sont moins. D'où l'importance pour ces dernières de renforcer leur dispositif de sécurité des systèmes d'information.

Photo de famille à l'issue de la Matinale organisée le 18 mars à Casablanca. Ph. Sradni

La situation a de quoi inquiéter. En ces temps de crise sanitaire, les cyber-attaques ont augmenté de 50% au Maroc. Avec l'accélération de la digitalisation du fait de cette crise, les cybercriminels ont intensifié leurs offensives, ciblant ainsi des pans stratégiques de l'économie nationale et internationale. Le constat est du Général de Brigade, Mostafa Rabii, directeur du Centre de veille de détection et de réponses aux cyber-attaques relevant de la Direction générale de la sécurité des systèmes d'information (DGSSI, Administration de la défense nationale). Il l'a partagé lors de son intervention à la 2e Matinale du Groupe Le Matin autour du thème «Cybersécurité : quelle protection dans un monde de plus en plus digitalisé?», organisée en partenariat avec Dell Technologies, le 18 mars à Casablanca.
Sans langue de bois, le Général de Brigade appelle vivement le monde des entreprises à la vigilance, surtout quand on sait que même les grandes structures dont la spécialité est la cybersécurité font l'objet d'attaques criminelles à l'instar de celle ayant ciblé Microsoft l'année dernière. «L'on est entré ainsi dans une atmosphère où l'on ne fait plus confiance aux grandes entités censées normalement nous protéger», souligne le Général de Brigade. Selon lui, le Maroc fait face, chaque jour, à des millions d'attaques, dont une dizaine qui réussit à menacer sérieusement les systèmes d'information du pays. «Parmi ces attaques, il y a celles qui sont bénignes et d'autres qui sont beaucoup plus dangereuses et que nous arrivons à bloquer. Celles-ci relèvent surtout du cyber-espionnage», explique le responsable. La montée en flèche des cyber-attaques dans le pays a été surtout favorisée par le recours intensif du télétravail. «Les sociétés n'étaient pas dûment outillées pour cette transition. Ce qui a offert une opportunité aux cyber-criminels», insiste Rabii.
Nawfal Saoud, general manager entreprise district Morocco chez Dell Technologies, reconnait également l'accroissement des cyber-attaques, pendant la crise sanitaire. «Nous avons constaté une montée dangereuse des cyber-attaques dans le contexte de la Covid-19. Ces menaces concernent pratiquement tous les secteurs», fait-il remarquer.

Les attaques de plus en plus sophistiquées

Saoud tire, par ailleurs, la sonnette d'alarme quant à la disposition des entreprises à faire face aux risques liés aux cyber-attaques. Concrètement, révèle-t-il, le Dell Global Index, dans sa version 2022, montre que 63% des entreprises sondées (sur un échantillon de 1.000 structures à travers le monde) déclarent être incapables d'être en conformité par rapport à la réglementation en vigueur dans leur secteur d'activité.
Autre conclusion, 61,2% de l'échantillon affirment être incapables de contrer une cyber-attaque de leurs systèmes d'information. Le fait est que, aujourd'hui, les attaques sont devenues tellement sophistiquées que les entreprises n'ayant pas investi suffisamment dans le renforcement de la sécurité de leur système d'information ne peuvent les bloquer. Salma Bennani, directrice Wavestone Maroc et spécialiste en transformation numérique et cybersécurité, a, pour sa part, révélé qu'en 2022, quelque 60 incidents majeurs impliquant carrément un arrêt d'activité de l'entreprise se sont produits. Encore une fois, c'est l'ensemble des secteurs économiques qui a été concerné. Et à Mostafa Rabii d'annoncer que, cette année, 490 entreprises ont été prévenues de cyber-attaques critiques dans des secteurs comme la santé, l'énergie ou l'enseignement.
Salma Bennani rejoint Nawfal Saoud et le Général de Brigade sur l'idée que les attaques sont devenues de plus en plus sophistiquées. Pour elle, la motivation derrière les cyber-attaques est la recherche de profit financier. D'ailleurs, poursuit-elle, 20% des entreprises ayant fait l'objet d'attaques cybercriminelles ont cédé aux Ransomwares. Une tendance que confirme le Général de Brigade à la Défense nationale qui souligne que les Ransomwares sont devenus de plus en plus dangereux, même s'ils ne sont pas très sophistiqués sur le plan technique. «Si les Ransomwares augmentent, c'est que les attaques qu'ils effectuent leur permettent de gagner de l'argent de manière facile. De même, cela leur permet de rester anonymes puisqu'ils encaissent les rançons en bitcoin. 90% des entités ayant été victimes de ces attaques payent les rançons de peur de perdre leur data», développe Rabii. Le responsable regrette, en outre, le fait que des entreprises ayant été victimes d'attaques ne veuillent pas faire leur déclaration auprès de la DGSSI.Intervenant à l'ouverture de la Matinale, Mohamed Haitami, PDG du Groupe Le Matin, a souligné, pour sa part, que «l'essor des monnaies cryptées, plus secures, intraçables et inviolables, a favorisé hélas les activités de Dark Web et le business des ransomwares». Haitami, qui cite un acteur mondial de la cybersécurité, indique que 13 millions d'attaques ont été détectés au Maroc entre avril et juin 2020, période de grand confinement et d'utilisation massive du digital suite à la propagation de la pandémie.
La transformation digitale est maintenant un fait. «Le débat sur son utilité n'a plus lieu d'être», a souligné pour sa part Omar Seghrouchni, président de la Commission nationale de contrôle de protection des données à caractère personnel (CNDP), qui est intervenu à distance. «Le risque 0 n'existant pas, résume le patron de la CNDP, les entreprises doivent se préparer que ce soit au niveau des ressources humaines et des compétences qu'au niveau des équipements. ■

Saïd Naoumi

> Cette année, 490 entreprises ont été prévenues de cyber-attaques critiques dans des secteurs comme la santé, l'énergie ou l'enseignement.
> **Mostafa Rabii**

Ph. Sradni

Ph. Sradni

Voir la vidéo sur lematin.ma

https://lematin.ma/qr/5414

Sécurité des SI : Pauvres investissements !

Les intervenants sont unanimes quant au renforcement de l'investissement des entreprises dans la composante sécurité des systèmes d'information. Pour Salma Bennani, les entreprises consacrent à peine 5% de leur budget SI à la sécurité. Mais lorsqu'un incident survient, les coûts peuvent s'avérer beaucoup plus lourds, dépassant de loin l'investissement qui devait normalement être dédié à la sécurité du système d'information. Mostafa Rabii confirme et révèle que ses services ont pu remonter l'exposition de 80 serveurs d'entreprises aux risques de cyber-attaques. Pourtant, 80% de ces entités n'ont pas procédé aux corrections nécessaires, faute de moyens financiers.
«Nous travaillons régulièrement avec l'administration publique, explique Rabii, afin d'imposer les corrections nécessaires des failles de leurs systèmes d'information. Avec le secteur privé, il est très difficile d'agir puisqu'on ne peut imposer ces paramétrages. Toutefois, nous sommes disposés à appuyer toute entreprise voulant renforcer son système de sécurité».

Matinales du Groupe Le Matin en partenariat avec Dell Technologies

Ils ont dit...

https://lematin.ma/qr/5418

Général de Brigade Mostafa Rabii, *directeur du Centre de veille de détection et de réponses aux cyberattaques relevant de la Direction générale de la sécurité des systèmes d'information-DGSSI, Administration de la Défense nationale*

La cybersécurité c'est d'abord la prévention et la capacité à prédire les cyberattaques. Pour cela, il est nécessaire de mener un travail d'évaluation et de veille en permanence pour pouvoir notamment détecter les vulnérabilités qui sont éventuellement exploitables par les hackers. L'idée donc est de sécuriser toute la chaîne et prendre toutes les dispositions pour ne pas être sujet à des cyberattaques. Aujourd'hui, l'intelligence artificielle aide aussi à la détection et donc permet une réaction rapide. Pour se protéger, il faut aussi des moyens techniques et des ressources humaines qualifiées, mais beaucoup d'institutions, qu'elles soient du secteur public ou privé, enregistrent un manque à ce niveau. C'est pour résoudre ce problème que la DGSSI a pensé à un système d'agréments, c'est-à-dire accréditer des sociétés pour faire de l'audit, de l'évaluation et offrir des services de SOC (Security Operation Center) incluant la prévention, l'analyse et la réaction. Cet agrément est un gage de confiance que l'on accorde à ces sociétés après de multiples tests pour mesurer leur compétences et fiabilité. Cette solution intéresse surtout les moyennes et petites entreprises qui n'ont pas les moyens pour s'offrir des systèmes sophistiqués de sécurité. Il faut noter que la DGSSI prend en charge la veille et la détection des cyberattaques au niveau des institutions de l'État, mais aussi des infrastructures d'importance vitales du secteur privé et public disposant de systèmes informatiques sensibles. Cette année, nous avons prévenu 490 entreprises de cyberattaques critiques dans des secteurs comme la santé, l'énergie ou l'enseignement.

https://lematin.ma/qr/5417

Nawfal Saoud, *General Manager Entreprise district Morocco chez Dell Technologies*

La cybersécurité est une thématique qui revêt aujourd'hui une importance stratégique pour les entreprises. Mais dans cet écosystème, nous constatons que le capital humain demeure l'élément faible de toute la chaîne et peut de ce fait mettre en péril la continuité du business d'une entreprise. De par notre interaction avec les entreprises, nous remarquons un manque de sensibilisation des utilisateurs/employés de l'entreprise, mais également un faible niveau d'investissement pour se procurer les ressources capables de gérer ce volet de la sécurité informatique. De ce fait, ces entreprises risquent fort de faire l'objet d'un nombre important de cyberattaques qui menaceraient la survie même de l'organisation. C'est pour ces raisons qu'au niveau de Dell Technologies, nous essayons de sensibiliser en faisant un focus sur le capital humain compétent pour accompagner les utilisateurs des systèmes d'information des entreprises. De plus, une attention particulière est portée aux équipes en charge de surveiller ces SI à travers des formations et en les dotant des équipements nécessaires pour assurer un niveau satisfaisant de sécurité de leurs systèmes d'information.

https://lematin.ma/qr/5416

Omar Seghrouchni, *président de la Commission nationale de contrôle de protection des données à caractère personnel-CNDP*

Le débat sur l'utilité de la digitalisation n'a plus lieu d'être. La transformation digitale est un fait, ce n'est plus un choix ou une option, et ce que nous vivons aujourd'hui en témoigne. Le débat est aujourd'hui ailleurs, il faut penser à mettre un code pour cette digitalisation, comment en tirer profit et éviter au maximum les risques qui lui sont liés, notamment les cyberattaques. Mais le risque zéro n'existe pas, les entreprises doivent se préparer, que ce soit au niveau des ressources humaines et des compétences ou au niveau des équipements. C'est un tout nouveau mode opératoire qu'il faut d'ores et déjà intégrer à la stratégie de gestion des entreprises, comme des administrations ou toute autre institution. En parallèle, il faut se focaliser sur la formation et la sensibilisation des usagers. Il faut en somme installer la digitalisation dans la culture de l'entreprise. Dans cet écosystème digital, il faut surtout veiller à protéger l'être humain et c'est dans ce sens que la protection des données personnelles est en phase d'évolution. En effet, la protection de la data a été perçue dans une dimension assez personnelle et limitée. Aujourd'hui, on doit gérer trois sommets d'un même triangle : 1. protéger la vie privée de la personne, 2. encourager l'économie numérique qui a besoin de ces données pour créer de la valeur ajoutée et de nouveaux usages, 3. favoriser la capacité de l'État à protéger les citoyens en tenant compte du rôle que joue désormais la data personnelle dans la gouvernance. En somme, on ne doit plus être dans une vision passive de la protection des données à caractère personnel, mais dans une vision dynamique et prospective en encourageant l'usage règlementé et structuré de la donnée.

https://lematin.ma/qr/5419

Salma Bennani, *directrice Wavestone Maroc et spécialiste en transformation numérique et cybersécurité*

Le Maroc a enregistré une réelle accélération des cyberattaques, notamment depuis la pandémie, et ce pour plusieurs raisons. Il s'agit d'abord de cette révolution digitale avec tout ce que cela implique au niveau des ouvertures des systèmes d'information. En plus, il y a le télétravail qui a augmenté les risques, au vu de la quantité de données qui circulent virtuellement. Ces ouvertures ont ainsi donné l'occasion aux cybercriminels d'attaquer beaucoup plus rapidement les données des entreprises et des personnes. Il est donc plus que jamais nécessaire que les entreprises et institutions investissent dans les équipements de sécurisation des données, mais aussi dans le capital humain compétent capable de faire de la veille et anticiper les cyberattaques. Il faut désormais des équipes qui travaillent sur les sujets de cybersécurité en entreprise, car c'est un domaine qui évolue très vite et qui nécessite une veille très dynamique. Les organisations gagneraient également à structurer leurs stratégies autour d'un programme de cybersécurité pour optimiser la sécurisation des données stratégiques. ■

Souad Badri