CybersÃ©curitÃ© : Ne plus nÃ©gliger la sÃ©curitÃ© des donnÃ©es
Internet
PostÃ© par : JulieM
PubliÃ©e le : 10/5/2021 13:00:00

Perte ou vol de donnÃ©es, usurpation dâidentitÃ© ou encore demande de ranÃ§on : la cybersÃ©curitÃ© est lâun des sujets au cÅur des prÃ©occupations de toutes les entreprises du monde, compte tenu du contexte de crise actuel. DÃ©sormais, elles doivent non seulement se protÃ©ger des attaques de hackers isolÃ©s mais aussi de bandes organisÃ©es, aux moyens financiers et technologiques consÃ©quents. Les enjeux sont rÃ©els : la pÃ©rennitÃ© et la rÃ©putation de lâorganisation attaquÃ©e.

Voici quelques conseils pour vÃ©ritablement se protÃ©ger de ces attaques, grÃ¢ce notamment Ã lâutilisation dâune plateforme de type Content Firewall.

Partager, câest crÃ©er une brÃ¨che

Lâobjectif des hackers est simple : exploiter au plus vite les vulnÃ©rabilitÃ©s des systÃ¨mes pour en prendre le contrÃ´le. Dans un monde de plus en plus collaboratif et basÃ© sur le tÃ©lÃ©travail, le partage dâinformations est vital. Sachant que tout peut arriver entre lâenvoi dâun fichier et sa rÃ©ception, il faut donc sÃ©curiser le processus.

Bien souvent, les applications business utilisÃ©es disponibles sur le marchÃ© ne sont pas sÃ©curisÃ©es en Â« natif Â» câest Ã dire pensÃ©es dÃ¨s la phase de conception et de dÃ©veloppement. Les couches de sÃ©curitÃ© sont ajoutÃ©es aprÃ¨s les couches fonctionnelles.

Les entreprises utilisent ces applications business pour partager de lâinformation avec leurs partenaires extÃ©rieurs (auditeurs, clients, fournisseurs, etcâ¦). Les hackers peuvent ainsi intercepter des informations et sâen servir pour mener des attaques de phishing ou de cyber-extorsion.

Mettre en place une plateforme sÃ©curisÃ©e dÃ©diÃ©e au partage dâinformations permet dâÃ©viter ce type dâattaques sous rÃ©serve de vÃ©rifier quâelle propose de vraies fonctions de sÃ©curitÃ© â MFA, chiffrement, mais aussi de lâIA pour alerter en temps rÃ©el lâÃ©quipe SOC.

Penser Â« donnÃ©es Â» avant tout

Une erreur courante en matiÃ¨re de sÃ©curitÃ© consiste Ã penser Ã lâenvironnement en premier lieu. GÃ©nÃ©ralement, les entreprises utilisent des solutions, des outils et des moyens pour se protÃ©ger Ã deux niveaux : le rÃ©seau et les applications, en oubliant souvent la protection des donnÃ©es â ce qui est paradoxal, sachant que la donnÃ©e est la cible finale de la majoritÃ© des attaques.

Les donnÃ©es se partagent et se stockent. Quel que soit le canal utilisÃ©, elles sont exposÃ©es dÃ¨s quâil y a partage, dâoÃ¹ la protection largement adoptÃ©e de leur environnement. Mais il ne suffit pas de protÃ©ger la donnÃ©e quand elle voyage, il faut aussi la protÃ©ger quand elle est stockÃ©e. Il est ainsi indispensable de sÃ©curiser ses donnÃ©es en permanence pour complÃ©ter les solutions de cybersÃ©curitÃ© dÃ©jÃ mises en place.

Pour cela, la meilleure approche est de se tourner vers une plateforme conÃ§ue pour prioriser la sÃ©curisation des donnÃ©es. Celle-ci a pour objectifs de prÃ©venir et rÃ©duire la surface dâattaque, puis accompagner les Ã©quipes en cas de problÃ¨me, en apportant notamment

visibilitÃ©, traÃ§abilitÃ©, et auditabilitÃ© des transactions et mouvements, Ã travers des logs et dashboards intÃ©grÃ©s.

Mettre lâ□□utilisateur au centre des prÃ©occupations

Se protÃ©ger des attaques extÃ©rieures ne doit pas devenir un parcours du combattant pour les utilisateurs, car sans leur adhÃ©sion au systÃ¨me mis en place, le risque de dÃ©faillance augmente â□□ le dÃ©veloppement du shadow IT par exemple. DÃ¨s lors, on distingue deux profils dâ□□utilisateurs.

Dâ□□une part, les Ã©quipes informatiques qui, grÃ¢ce Ã la plateforme choisie, vont consolider les besoins en matiÃ¨re de sÃ©curitÃ©. Disposer dâ□□une seule solution centralisÃ©e favorise le gain de temps et de ressources au niveau des DSI et des opÃ©rationnels de lâ□□IT. Cela se traduit notamment dans lâ□□intÃ©gration de ladite plateforme au systÃ¨me dâ□□information existant et son exploitation par la suite.

Ils sâ□□assureront quâ□□elle soit simple dâ□□implÃ©mentation et de mise en Å□uvre mais surtout compatible avec tous les types de dÃ©ploiement (on premise, Cloud, multi-cloud, hybride) et avec les partenaires technologiques tel que Google ou Microsoft, pour nâ□□en citer que deux. Ils veilleront Ã©galement Ã la prÃ©sence dâ□□un Bug Bounty Program et de Pentests rÃ©guliers et systÃ©matiques dans le cycle de dÃ©veloppement produit du fournisseur. A noter, la validation de chaque version doit Ãªtre effectuÃ©e par un RSSI (CISO) certifiÃ©.

Dâ□□autre part, les utilisateurs au sein de lâ□□organisation qui ont besoin dâ□□un accÃ¨s simple, et dâ□□une exploitation facile et fluide. La plateforme doit donc Ãªtre accessible depuis nâ□□importe quel navigateur et lâ□□existence de plugins disponibles pour les logiciels et applications les plus populaires sont un rÃ©el atout supplÃ©mentaire pour rendre lâ□□expÃ©rience utilisateur intuitive.

De la mÃªme faÃ§on, pour adresser lâ□□ensemble des besoins de lâ□□entreprise, la plateforme doit Ãªtre capable de proposer Ã lâ□□utilisateur un espace permettant par exemple dâ□□envoyer ses emails de faÃ§on sÃ©curisÃ©e ou de partager des fichiers en utilisant directement le navigateur dÃ©ployÃ© dans lâ□□entreprise.

Compte tenu de lâ□□augmentation exponentielle des attaques et de lâ□□importance de se protÃ©ger contre celles-ci, les entreprises doivent aujourdâ□□hui changer de paradigme et passer Ã une stratÃ©gie de sÃ©curitÃ© offensive. La plupart des applications quâ□□elles utilisent, bien que sÃ©curisÃ©es et fiables Ã un instant donnÃ©, ne le sont pas forcÃ©ment sur le long terme.

Tout systÃ¨me, quel quâ□□il soit, est vulnÃ©rable et les hackers le savent mieux que personne. Il faut donc que la sÃ©curitÃ© soit intÃ©grÃ©e sur lâ□□ensemble du cycle de vie dâ□□une solution, de la conception au dÃ©veloppement - quitte Ã imposer des formations spÃ©cifiques aux Ã©quipes dÃ©diÃ©es - jusquâ□□Ã sa mise en production, puis dans le suivi des vulnÃ©rabilitÃ©s. Lâ□□objectif principal est de dÃ©jouer, le plus tÃ´t possible, les attaques de type zero-day, qui exploitent les vulnÃ©rabilitÃ©s non corrigÃ©es.

Philippe Perrin, Country Manager Accellion