Cyberattaques : Se protÃ©ger de faÃ§on simple et durable ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 25/3/2022 15:00:00

Bien que les techniques de dÃ©veloppement logiciel et les bonnes pratiques aient Ã©voluÃ© en termes de sÃ©curitÃ©, il reste impossible de garantir l'absence de vulnÃ©rabilitÃ©s. Leur correction fait partie intÃ©grante du cycle de vie des solutions.

En 2021, de nombreux Ã©vÃ©nements de sÃ©curitÃ© ont exploitÃ© des vulnÃ©rabilitÃ©s bien connues et certaines souvent anciennes.

Aussi, le principal enjeu en termes de cybersÃ©curitÃ© consiste Ã protÃ©ger ses actifs au sein d'un rÃ©seau privÃ© virtuel sÃ©curisÃ© et Ã maintenir toutes les composantes du systÃ¨me d'information dans des conditions optimales de sÃ©curitÃ©.

Parmi celles qui nÃ©cessitent une attention maximale, l'ANSSI met l'accent sur les passerelles VPN qui permettent d'accÃ©der au systÃ¨me d'information depuis l'Internet.

Ces solutions doivent Ãªtre mises Ã jour trÃ¨s rapidement et les mÃ©canismes d'authentification et de transport doivent Ãªtre particuliÃ¨rement robustes (MFA, chiffrement, historisation). Ces opÃ©rations sont sensibles et doivent Ãªtre correctement rÃ©alisÃ©es pour limiter les risques d'impact sur la production.

Le modÃ¨le SASE [Secure Access Service Edge] dÃ©fini par GARTNER aide clairement les organisations dans ce travail vital, complexe et coÃ»teux.

Le SASE consiste Ã sâ□□appuyer sur une architecture rÃ©seau et sÃ©curitÃ© de nouvelle gÃ©nÃ©ration dÃ©livrÃ©e dans le Cloud. Elle permet aux organisations de connecter de faÃ§on sÃ©curisÃ©e nâ□□importe quel utilisateur Ã nâ□□importe quelle application, partout dans le monde.

Les entreprises peuvent alors mener Ã bien la mutation de leurs infrastructures rÃ©seau et sÃ©curitÃ© pour rÃ©ussir leur transformation numÃ©rique. Il sâ□□agit dâ□□un dispositif unique qui permet aux Ã©quipes de travailler en toute sÃ©curitÃ© en sâ□□appuyant sur des infrastructures Ã hautes performances.

Par ailleurs, face Ã lâ□□exposition aux cybermenaces, le rÃ©flexe de beaucoup dâ□□organisations est dâ□□accroitre le nombre dâ□□outils de sÃ©curitÃ©.
Une Ã©tude rÃ©cente a montrÃ© que ceux-ci ont augmentÃ© de prÃ¨s de 20% depuis 2019.

Le mieux Ã©tant souvent lâ□□ennemi du bien, cette approche provoque lâ□□effet contraire de celui escomptÃ©. Car au-delÃ de la fuite en avant financiÃ¨re, lâ□□empilement des outils augmente la complexitÃ©.

Les Ã©quipes IT ou leurs prestataires doivent rÃ©aliser des efforts dâ□□intÃ©gration et de maintien en conditions opÃ©rationnelles trÃ¨s importants.

Ceci requiert une expertise et une charge trÃ¨s consÃ©quente pour un rÃ©sultat souvent hypothÃ©tique, car :

â¢ Comment collecter et corrÃ©ler efficacement les informations provenant de sources et de formats multiples ?
â¢ Comment Ã©valuer leur pertinence et identifier avec prÃ©cision les faux positifs ?
â¢ Comment sâassurer que les outils fonctionnent correctement ensemble alors quâils doivent Ãªtre en permanence mis-Ã -jour ?

Et finalement, ces outils contribuent-ils vraiment Ã une posture de sÃ©curitÃ© efficace et pÃ©renne ?

Pour preuve, les marqueurs prÃ©curseurs dâune attaque sont prÃ©sents au sein du SystÃ¨me dâInformation des semaines voire des mois avant la concrÃ©tisation de leurs actions.
Pendant cette pÃ©riode, les Ã©quipes IT disposent de nombreuses possibilitÃ©s de dÃ©tecter, limiter, voire juguler lâattaque en identifiant les opÃ©rations en cours de rÃ©alisation :
â¢ Collecte de mots de passe
â¢ ExÃ©cution dâoutils systÃ¨mes
â¢ Modification des privilÃ¨ges, dÃ©placement latÃ©ral vers des donnÃ©es Ã valeur ajoutÃ©e, ou encore mise en place de tunnels dâexfiltration

Pourtant dans la majoritÃ© des cas, ces signaux Ã©chappent aux contrÃ´les de sÃ©curitÃ© en place.

Alors, plutÃ´t que de tenter dâajouter en permanence de nouvelles fonctions de dÃ©fense, il est plus utile de se concentrer sur lâutilisation efficace de solutions simples.

Car peu importe comment les attaquants ont pÃ©nÃ©trÃ© le SystÃ¨me dâInformation. Leur agilitÃ© leur permettra toujours de trouver le moyen dây parvenir.
Ce qui est important câest de contrer ce quâils sont venus y faire.
Et sur ce point, les attaquants ont toujours les mÃªmes objectifs : hameÃ§onnage, vol de mots de passe, analyse des vulnÃ©rabilitÃ©s.

Lâempilement des solutions de sÃ©curitÃ© apporte donc plus de complexitÃ© que dâefficacitÃ© dans la cyberdÃ©fense des organisations.
Il est plus utile de capitaliser sur des solutions simples et bien maÃ®trisÃ©es par les Ã©quipes IT.

Cette approche basÃ©e sur la simplicitÃ© et lâefficacitÃ© de la sÃ©curitÃ© est lâun des piliers du modÃ¨le SASE.

Dans ce modÃ¨le, les fonctions de sÃ©curitÃ© essentielles contre les intrusions et les logiciels malveillants :

â¢ Sont dÃ©livrÃ©es dans le Cloud et nâont aucune empreinte sur le SystÃ¨me dâinformation, ce qui simplifie leur mise en Åuvre
â¢ Couvrent tous les actifs et les modes de travail
â¢ Sont mises Ã jour automatiquement par lâÃ©diteur sans action nÃ©cessaire des Ã©quipes IT
â¢ Unifient tous les Ã©vÃ©nements de sÃ©curitÃ© pour permettre une analyse directe et efficace

Les bÃ©nÃ©fices sont alors mesurables Ã diffÃ©rents niveaux :

- RÃ©duction de la surface d'attaque du SystÃ¨me d'Information
- Protection temps rÃ©el et 0-day contre les intrusions et les logiciels malveillants
- Ãlimination de la charge et des risques associÃ©s aux mises Ã jour de sÃ©curitÃ©
- ContrÃ´le des accÃ¨s aux applications internes et Cloud rÃ©alisÃ©s par les utilisateurs sur site ou en situation de mobilitÃ©

- Historisation de tous les Ã©changes

En conclusion, la rÃ©duction du risque dâ□□exposition aux cyberattaques repose sur des solutions simples Ã dÃ©ployer et Ã opÃ©rer. Le modÃ¨le SASE constitue vÃ©ritablement aujourdâ□□hui le socle pÃ©renne de la performance et de la sÃ©curitÃ© IT des entreprises.

Plus tÃ´t elles amorceront son adoption, plus vite elles pourront rÃ©pondre efficacement aux enjeux digitaux de leurs mÃ©tiers et aux nouveaux modes de production de leurs collaborateurs.

Â JÃ©rÃ´me BEAUFILS, PrÃ©sident de Sasety