***Recommandations en matiÃ¨re de cybersÃ©curitÃ©***
**Internet**
PostÃ© par : JulieM
PubliÃ©e le : 28/1/2022 13:00:00

Lâ□□annÃ©e 2021 a Ã©tÃ© marquÃ©e par une augmentation du nombre de failles de sÃ©curitÃ© trÃ¨s mÃ©diatisÃ©es, dont beaucoup se sont soldÃ©es par des attaques de ransomware dÃ©vastatrices.

Les cybercriminels ont ainsi frappÃ© des cibles traditionnellement plus faciles Ã  atteindre - comme les hÃ´pitaux, les Ã©coles et les collectivitÃ©s locales - tout en continuant Ã  sâ□□intÃ©resser Ã  la supply chain. Bien que la cause profonde de ces cyberattaques varie, toutes ont tirÃ© parti dâ□□une authentification Ã  facteur unique, dâ□□une authentification multifacteurs faible (OTP, par exemple) ou de secrets exposÃ©s (clÃ©s de signature SAML, par exemple).

En 2022, Chad Thunberg, RSSI de Yubico, prÃ©voit sur une poursuite de lâ□□extorsion des victimes via des ransomwares, en raison du succÃ¨s rencontrÃ© par ces campagnes en 2021. En outre, une attention particuliÃ¨re devrait Ãªtre accordÃ©e aux rÃ©glementations, afin dâ□□accÃ©lÃ©rer la concrÃ©tisation des pratiques et des principes de sÃ©curitÃ© de lâ□□information dans les secteurs vulnÃ©rables.

### 1. Placer lâ□□architecture Â« Zero Trust Â» comme une prioritÃ©

Lâ□□incident de SolarWinds et la rÃ©cente vulnÃ©rabilitÃ© de Log4j ont mis en Ã©vidence que les systÃ¨mes internes critiques de certaines entreprises offrent un accÃ¨s permissif Ã  internet et Ã  des systÃ¨mes non fiables, alors que lâ□□application du principe du moindre privilÃ¨ge et la segmentation sont prÃ©conisÃ©s depuis des dÃ©cennies.

Les modÃ¨les de sÃ©curitÃ© de type Â« Zero Trust Â» font progresser le dÃ©bat, mais en modifiant fondamentalement lâ□□approche de la sÃ©curitÃ© de lâ□□information. Au lieu de supposer que lâ□□environnement interne est digne de confiance, ce modÃ¨le part en effet du principe quâ□□il est hostile.

La confiance est alors instaurÃ©e au moyen dâ□□une inspection et dâ□□une authentification forte, mais elle reste Ã©phÃ©mÃ¨re dans la mesure oÃ¹ elle doit Ãªtre rÃ©tablie Ã  intervalles rÃ©guliers. En thÃ©orie, cette approche devrait limiter les violations rÃ©ussies en rÃ©duisant la fenÃªtre dâ□□opportunitÃ© et en renforÃ§ant lâ□□isolement.

### 2. Adopter une authentification multifacteur (MFA) rÃ©sistant au phishing

Le phishing, le credential stuffing et dâ□□autres menaces relatives Ã  lâ□□authentification par mot de passe, continueront Ã  faire peser un risque important sur les entreprises. Les cybercriminels ont dÃ©montrÃ© quâ□□ils Ã©taient capables dâ□□accÃ©der aux rÃ©seaux internes au sein desquels lâ□□authentification Ã  facteur unique et la MFA faible sont encore prÃ©dominantes.

GrÃ¢ce aux identifiants volÃ©s, les hackers ont la possibilitÃ© de se maintenir dans lâ□□environnement sans avoir Ã  exploiter les vulnÃ©rabilitÃ©s ou Ã  effectuer dâ□□autres actions qui augmenteraient la probabilitÃ© de dÃ©tection.

### 3. Surmonter la peur du Cloud

Des entreprises et des secteurs continuent de percevoir le cloud comme une menace, en raison essentiellement dâ□□un sentiment de maintien du contrÃ´le en termes de sÃ©curitÃ©. Or, le cloud offre un ensemble solide de fonctions et de protocoles de sÃ©curitÃ©.

Lorsque ceux-ci sont utilisÃ©s de maniÃ¨re adÃ©quate, la plupart des menaces auxquelles les organisations sont confrontÃ©es aujourdâ□□hui, comme les ransomwares et la compromission des courriers Ã©lectroniques professionnels, sont largement attÃ©nuÃ©es.

La combinaison de lâ□□identitÃ© fÃ©dÃ©rÃ©e, de lâ□□authentification multifacteurs forte et du stockage de fichiers dans le cloud, reprÃ©sente donc un atout majeur pour les entreprises de toutes tailles.

Lâ□□authentification et le chiffrement mutuels par TLS peuvent gÃ©nÃ©ralement Ãªtre activÃ©s en cochant une simple case, les complexitÃ©s des ICP (infrastructure Ã clÃ©s publiques) Ã©tant gÃ©rÃ©es et automatisÃ©es en arriÃ¨re-plan. Une surveillance et un contrÃ´le supplÃ©mentaires sont Ã©galement possibles pour les entreprises qui sont intÃ©ressÃ©es par la gestion de leurs propres secrets et qui sont suffisamment matures pour le faire.

Il nâ□□est pas nÃ©cessaire dâ□□adopter le cloud pour bÃ©nÃ©ficier des avantages de lâ□□identitÃ© fÃ©dÃ©rÃ©e et de lâ□□authentification multifacteurs forte. La plupart des offres modernes de fournisseurs dâ□□identitÃ© prennent en charge les protocoles FIDO, SAML et OpenID Connect pour faciliter lâ□□intÃ©gration des applications sur site et hors site.

### 4. Se prÃ©parer aux ransomwares

Les organisations dotÃ©es de modÃ¨les de pÃ©rimÃ¨tre traditionnels et dâ□□une infrastructure classique reposant sur des technologies telles que lâ□□Active Directory doivent Ã©tablir un plan dâ□□intervention solide pour faire face aux attaques par ransomware.

Le plan doit aborder des sujets qui vont au-delÃ de la dÃ©tection et de la rÃ©cupÃ©ration, comme la couverture dâ□□assurance, la consultation externe et les mesures Ã prendre pour payer la ranÃ§on si la rÃ©cupÃ©ration Ã©choue. Les polices dâ□□assurance peuvent couvrir le coÃ»t de lâ□□embauche dâ□□un tiers, mais uniquement lorsquâ□□un fournisseur agrÃ©Ã© est utilisÃ©.

La couverture peut Ã©galement Ãªtre soumise Ã des limites. RÃ©cemment, il a Ã©tÃ© constatÃ© des modifications de la couverture selon que lâ□□attaquant est un Ã□tat-nation ou non. En outre, une fois le plan mis en place, il faut le tester, notamment les sauvegardes Ã©ventuelles.

### 5. SÃ©curiser la supply chain

En 2021, lâ□□incident de SolarWinds et la vulnÃ©rabilitÃ© de log4j nous ont non seulement fait prendre conscience de la fragilitÃ© des supply chains, mais ont Ã©galement mis en Ã©vidence le fait que les systÃ¨mes critiques et hautement sensibles ont toujours la possibilitÃ© de se connecter arbitrairement Ã des systÃ¨mes non fiables sur Internet.

Toutes les organisations doivent donc prendre conscience quâ□□il est de leur responsabilitÃ© mutuelle de garantir la sÃ©curitÃ© de la conception, du dÃ©veloppement et de lâ□□exploitation des technologies. Le processus dâ□□assurance des fournisseurs, parsemÃ© de questionnaires non standardisÃ©s, ne peut Ã lui seul sÃ©curiser la supply chain.

Les entreprises intervenant dans une supply chain devront instaurer une confiance mutuelle, Ã©tablie par la mise en Å□uvre de bonnes pratiques en matiÃ¨re de cybersÃ©curitÃ© tout au long de leur processus de dÃ©veloppement, et se montrer capables dâ□□en faire la dÃ©monstration.

Dans lâ□□idÃ©al, lâ□□ensemble du processus de dÃ©veloppement, de la validation du code Ã sa

publication, devrait Ãªtre sÃ©curisÃ© par une authentification forte, des contrÃ´les dâintÃ©gritÃ© solides et des modÃ¨les dâautorisation Ã  moindre privilÃ¨ge.

Les entreprises qui mettent en Åuvre cette technologie doivent suivre les pratiques reconnues par lâindustrie (par exemple, le Â« Zero Trust Â») pour assurer la sÃ©curisation de la technologie par la segmentation, lâapplication de correctifs et des modÃ¨les de contrÃ´le dâaccÃ¨s rÃ©silients.

### 6. Prioriser la protection de la vie privÃ©e des utilisateurs

Selon de rÃ©centes prÃ©visions de Gartner, dâici fin 2023, les lÃ©gislations modernes sur la protection de la vie privÃ©e couvriront les informations personnelles de 75 % de la population mondiale.

Ã mesure que des lÃ©gislations similaires au RGPD continueront dâÃªtre mises en Åuvre dans le monde pour protÃ©ger la sÃ©curitÃ© et Ã  la vie privÃ©e de millions de citoyens, le nouveau problÃ¨me auquel les organisations seront confrontÃ©es sera la gestion de multiples lÃ©gislations sur la protection des donnÃ©es dans diverses juridictions.

Les entreprises doivent protÃ©ger les informations rÃ©glementÃ©es tout au long de leur cycle de vie et pas seulement au point dâentrÃ©e. Bien que le RGPD nâimpose pas dâexigences en matiÃ¨re dâauthentification, nous nous attendons Ã  voir apparaÃ®tre de plus en plus dâexigences prescriptives Ã  mesure que dâautres juridictions Ã©laboreront leurs propres ensembles dâexigences.Â