CybersÃ©curitÃ© & DevOps en 2018 : lâ□□annÃ©e du changement ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 17/1/2018 13:00:00

Le dÃ©but de lâ□□annÃ©e 2018 commence fort en matiÃ¨re de cybermenaces avec la dÃ©couverte des vulnÃ©rabilitÃ©s Meltdown et Spectre visant les processeurs Intel. Une nouvelle preuve, sâ□□il en fallait, que si les attaques mondiales WannaCry et NotPetya survenues lâ□□an passÃ© ont sensibilisÃ©, elles nâ□□ont toutefois pas permis dâ□□Ã©radiquer les mauvaises pratiques.

Or, la thÃ©orie est toujours plus aisÃ©e que la rÃ©alitÃ©, et la faille Intel dÃ©montre que la vulnÃ©rabilitÃ© nâ□□est dÃ©cidÃ©ment jamais oÃ¹ on lâ□□attend et que les cyberpirates continuent de garder une longueur dâ□□avance.

Dans ce contexte dâ□□hypersensibilisation, Elizabeth Lawler, Vice President of DevOps Security, chez CyberArk, estime quâ□□au niveau des DevOps â□□ soit le mÃ©lange des tÃ¢ches qu'effectuent les Ã©quipes d'une entreprise chargÃ©es du dÃ©veloppement des applications et de l'exploitation des systÃ¨mes[1] â□□ trois tendances domineront lâ□□annÃ©e 2018 :

Â« Tout dâ□□abord, lâ□□attaque contre Uber ne sera pas la derniÃ¨re. En effet, bien quâ□□elle ait fait la une des media, cette faille nâ□□aurait pas dÃ» Ã©tonner autant : les donnÃ©es de 57 millions de clients ont Ã©tÃ© piratÃ©es car les dÃ©veloppeurs de lâ□□entreprise exposaient des secrets au sein de solutions de stockage de codes publiques.

Cela a notamment permis aux hackers d'accÃ©der aux comptes Ã privilÃ¨ges dâ□□Uber. La raison de cette pratique sensible ? Il n'existe tout simplement pas de moyens simples et sÃ©curisÃ©s pour que les diffÃ©rents dÃ©partements dâ□□une entreprise collaborent.

De nombreuses organisations ne parviennent ainsi pas Ã sÃ©curiser les activitÃ©s des spÃ©cialistes DevOps, ce qui provoque des tensions et des vulnÃ©rabilitÃ©s. Les dÃ©veloppeurs ne sont pas, et ne devraient pas, Ãªtre des employÃ©s chargÃ©s de la sÃ©curitÃ©. Ils sont en effet responsables des caractÃ©ristiques et des fonctionnalitÃ©s, et non de la gestion de la collaboration et de la sÃ©curisation des identifiants.

Une Ã©tude rÃ©cente de CyberArk indique que la plupart des organisations franÃ§aises ne

connaissent pas tous les lieux et les outils dans lesquels les identifiants sont stockÃ©s. Ces entreprises sont par consÃ©quent trÃ¨s vulnÃ©rables, et plus de 79 % dâ□□entre elles n'ont aucune stratÃ©gie pour y remÃ©dier. Câ□□est pourquoi il est fort probable que les attaques continueront dâ□□aboutir en 2018, et au-delÃ .

Lâ□□Ã©chec est Ã©vident lorsquâ□□on demande Ã un employÃ© de gÃ©rer la sÃ©curitÃ©, alors que cela ne fait pas partie de ses prÃ©rogatives et qu'il ne possÃ¨de pas d'expÃ©rience en la matiÃ¨re. L'automatisation a cependant un rÃ´le clÃ© Ã jouer dans l'amÃ©lioration de la sÃ©curitÃ©, en lâ□□intÃ©grant Ã l'expÃ©rience native des dÃ©veloppeurs.

En outre, lâ□□attaque dâ□□Uber n'aurait pas dÃ» Ãªtre si singuliÃ¨re car de nouvelles recherches indiquent que lâ□□entreprise est loin dâ□□Ãªtre un cas isolÃ©, avec 62 % des organisations franÃ§aises qui nâ□□auraient pas informÃ© leurs clients de la compromission de leurs donnÃ©es personnelles lors d'une cyberattaque. Quoiquâ□□alarmant, ce constat nâ□□est pas surprenant.

Cette annÃ©e, les spÃ©cialistes DevOps seront de plus surchargÃ©s et nous constaterons un nouveau manque de talents DevSecOps. Les organisations se tournent ainsi de plus en plus vers les workflows DevOps pour atteindre une rapiditÃ© dâ□□exÃ©cution et dâ□□innovation. Elles ne sont cependant pas prÃ©parÃ©es ou dotÃ©es du personnel adÃ©quat pour gÃ©rer la sÃ©curitÃ© de ces environnements.

2018 verra donc un manque critique de spÃ©cialistes DevSecOps â□□ qui intÃ¨grent la cybersÃ©curitÃ© tout au long du cycle de vie dâ□□une application â□□ alors mÃªme que la protection devient une prioritÃ© pour les entreprises. Actuellement, beaucoup dâ□□entre elles la confient dÃ©jÃ aux spÃ©cialistes DevOps, en sus des nombreuses responsabilitÃ©s qui leur incombent, et ce malgrÃ© leur manque dâ□□expÃ©rience en la matiÃ¨re.

Mais cela doit cesser, surtout si on considÃ¨re l'augmentation de la surface dâ□□attaque Ã©tendue dans les workflows DevOps, ainsi que les risques associÃ©s Ã la gestion des scripts, des plateformes et des systÃ¨mes utilisÃ©s dans les workflows automatisÃ©s.

Les experts DevSecOps sont donc trÃ¨s demandÃ©s, et les profils manqueront en 2018, puisque les organisations rÃ©alisent que mÃªme si elles ont les bons outils, elles n'ont pas nÃ©cessairement les bonnes personnes pour les gÃ©rer. La sÃ©curitÃ© deviendra un travail Ã temps plein, axÃ© sur les workflows DevOps, et il y aura peu de personnes disponibles pour mener Ã bien ces missions.

Enfin, en 2018, le moindre privilÃ¨ge fera peau neuve dans lâ□□univers DevOps. Les entreprises commencent en effet Ã comprendre que Â« lâ□□identitÃ© Â» n'a, jusquâ□□ici, pas Ã©tÃ© complÃ¨tement prise en compte ; il n'y a pas de standard commun pour l'identitÃ© machine, le contrÃ´le et la gestion des accÃ¨s, ou encore l'audit sur lâ□□ensemble des composants de la plateforme.

Les organisations sont donc aussi vulnÃ©rables que leur Ã©lÃ©ment le plus faible. Ce dernier peut Ãªtre une machine virtuelle, un conteneur ou l'une des dizaines de couches de plateforme qui existent dÃ©sormais sur un rÃ©seau. Et lorsque ces matrices sâ□□Ã©tendent, elles deviennent beaucoup plus difficiles Ã contrÃ´ler.

Par consÃ©quent, la cybersÃ©curitÃ© nÃ©cessite une dÃ©finition plus prÃ©cise de l'identitÃ© machine dans les systÃ¨mes hautement automatisÃ©s, qui transportent des donnÃ©es de plus en plus sensibles. DÃ¨s l'annÃ©e 2018, les concepts prÃ©cÃ©demment utilisÃ©s dans la gestion de l'accÃ¨s humain, seront appliquÃ©s aux machines de maniÃ¨re significative.

En forÃ§ant les spÃ©cialistes DevOps Ã poser aux machines la question "qui Ãªtes-vous, qu'est-ce que vous Ãªtes et que souhaitez-vous ?", et ce y compris dans l'environnement DevOps, les

organisations pourront appliquer de meilleures pratiques de sÃ©curitÃ© et limiter les activitÃ©s des machines, sans compromettre pour autant les opÃ©rations.

Cela permettra une vÃ©ritable responsabilisation de la sÃ©curitÃ© des environnements DevOps, et le processus de livraison continue du moindre privilÃ¨ge des DevSecOps pourra devenir une rÃ©alitÃ©. Â»

Elizabeth Lawler, Vice President of DevOps Security chez CyberArk