La cybersÃ©curitÃ© nâ□□est pas quâ□□une affaire de technologies
Internet
PostÃ© par : JerryG
PubliÃ©e le : 4/5/2022 15:00:00

Outre le vol de donnÃ©es ou dâ□□argent, le plus grand impact des attaques de trÃ¨s grande ampleur comme celles de SolarWinds, Colonial Pipeline et Log4j est que lâ□□on commence Ã prendre conscience que les cyberattaques et les cyber dommages sont inÃ©vitables.

Cependant, bien que les fraudeurs aient toujours Ã©tÃ© aussi omniprÃ©sents que la mort et les impÃ´ts, il est possible de rÃ©duire la frÃ©quence et la rÃ©ussite de ces incidents, et dâ□□en contrÃ´ler lâ□□impact.

En dÃ©pit de ce que vous diront la plupart des Ã©diteurs et experts, la rÃ©ponse nâ□□est pas simplement Â« dâ□□acheter plus dâ□□outils Â». Bien que les technologies et les outils jouent un rÃ´le prÃ©cieux dans la protection des organisations, on nâ□□Ã©voque pas assez souvent les solutions Â« non techniques Â» Ã la disposition des organisations cherchant Ã renforcer leur sÃ©curitÃ©.

Fort dans mon expÃ©rience en tant que RSSI et dans la rÃ©ponse aux incidents, je souhaite offrir mes conseils quant aux mesures que les Ã©quipes informatiques opÃ©rationnelles et de sÃ©curitÃ© devraient prendre en compte pour reprendre le contrÃ´le et adopter une approche plus proactive.

Les meilleures pratiques Ã envisager

BÃ¢tir une Ã©quipe diversifiÃ©e

Le secteur de la sÃ©curitÃ© est marquÃ© par une forte homogÃ©nÃ©itÃ©. Les femmes ne constituent ainsi que 20% du personnel dans la sÃ©curitÃ© informatique. Les femmes et les groupes minoritaires sont largement sous-reprÃ©sentÃ©s dans ce domaine, et il faut que cela change, non seulement pour remÃ©dier Ã la pÃ©nurie de compÃ©tences, mais aussi pour crÃ©er des Ã©quipes plus performantes.

Mieux vaut Ã©viter de se retrouver avec un groupe de personnes partageant le mÃªme mode de pensÃ©e. En intÃ©grant un groupe de personnes plus diversifiÃ©, vous aurez plus de perspectives - des personnes qui remettront en question vos hypothÃ¨ses et introduiront de nouvelles faÃ§ons de penser. Dans un domaine en Ã©volution constante comme la cybersÃ©curitÃ©, c'est exactement ce dont vous avez besoin.

Cet effort doit commencer avec le processus de recrutement : cherchez dâ□□abord Ã crÃ©er un pipeline de talents diversifiÃ© (genre, Ã¢ge, expÃ©rience, formation, rÃ©gion gÃ©ographique etc.). Et si vous vous accrochez encore Ã la peur de Â« passer Ã cÃ´tÃ© Â» de candidats plus qualifiÃ©s en faisant de la diversitÃ© une de vos prioritÃ©s, il est temps de lÃ¢cher prise.

Il existe une plÃ©thore de candidats incroyablement qualifiÃ©s dans les catÃ©gories sous-reprÃ©sentÃ©es â□□ il vous suffit de faire un petit effort pour les trouver.

Enfin, rÃ©flÃ©chissez Ã la nÃ©cessitÃ© dâ□□embaucher des spÃ©cialistes de la sÃ©curitÃ© (des individus disposant dâ□□une expÃ©rience ou des diplÃ´mes adÃ©quats) ; ou Ã la possibilitÃ© de faire appel Ã des profils capables de sâ□□adapter et de faire preuve de sens critique, et de leur

dispenser la formation adÃ©quate.

Ã□largissez les critÃ¨res de ce que vous considÃ©rez comme un candidat Â« qualifiÃ© Â», en particulier pour les postes de dÃ©butant, afin de profiter dâ□□une main-dâ□□Å□uvre bien plus diversifiÃ©e.

Ne pas hÃ©siter Ã externaliser

La pÃ©nurie de compÃ©tences dans le domaine de la cybersÃ©curitÃ© est Ã©voquÃ©e depuis de nombreuses annÃ©es. Et malheureusement, elle nâ□□a de cesse de sâ□□accentuer. Selon Cybersecurity Ventures, le nombre de postes non pourvus dans le domaine de la cybersÃ©curitÃ© unifiÃ©e Ã©tait censÃ© atteindre les 3,5 millions fin 2021.

Je sais que les spÃ©cialistes de la sÃ©curitÃ© sont rÃ©putÃ©s pour leur paranoÃ¯a et leur mÃ©fiance â□□ ces caractÃ©ristiques sont souvent bÃ©nÃ©fiques dans notre mÃ©tier â□□ et veulent gÃ©rer un maximum de tÃ¢ches en interne. Mais mon conseil, notamment pour les petites entreprises, est dâ□□envisager sÃ©rieusement la possibilitÃ© de faire appel Ã un fournisseur de services externe pour renforcer leur Ã©quipe.

Face au manque de personnel informatique et de sÃ©curitÃ©, ces MSP reprÃ©sentent donc une bonne opportunitÃ©. Lâ□□essentiel est de veiller Ã contrÃ´ler soigneusement leurs antÃ©cÃ©dents et Ã obtenir des recommandations Ã leur Ã©gard, afin de sâ□□assurer que le prestataire choisi propose une offre de sÃ©curitÃ© Ã©prouvÃ©e â□□ tout en conservant suffisamment de professionnels talentueux en interne pour superviser vos services externalisÃ©s.

Sâ□□entraÃ®ner comme pour le jour J

Si les outils sont importants, rien ne remplace la formation de votre personnel. Fort de mon expÃ©rience en tant quâ□□ingÃ©nieur et enquÃªteur en cybersÃ©curitÃ© au dÃ©but de ma carriÃ¨re, et maintenant en tant que responsable, je sais quâ□□il faut sâ□□entraÃ®ner comme si lâ□□on Ã©tait le jour J, et rÃ©pÃ©ter le jour J ce Ã quoi on sâ□□est entraÃ®nÃ©.

Les compÃ©tences les plus essentielles Ã dÃ©velopper sont la capacitÃ© de rÃ©ponse aux incidents et de gestion des crises. Pour vous aider, diffÃ©rentes mÃ©thodes dâ□□entraÃ®nement â□□ Ã©quipes rouges/bleues, CTF (capture de drapeau) et exercices de simulation â□□ sont Ã votre disposition.

Outre le fait de tester les capacitÃ©s de sÃ©curitÃ© de votre organisation, ces exercices peuvent vous en apprendre beaucoup sur votre Ã©quipe. Qui tire son Ã©pingle du jeu sous la pression ? Qui montre les caractÃ©ristiques dâ□□un leader ? Comment votre Ã©quipe sâ□□adapte-t-elle et communique-t-elle lorsquâ□□elle est confrontÃ©e Ã des obstacles ?

Mais surtout, quelles sont les lacunes de vos plans actuels ? Partant de ces enseignements, vous pourrez organiser votre Ã©quipe de faÃ§on Ã Ãªtre idÃ©alement prÃ©parÃ© dans le cas oÃ¹ une attaque se produirait.

Les postulats Ã (rÃ©)Ã©valuer

Les trois points ci-dessus sont des pratiques susceptibles de permettre aux organisations de renforcer leur cybersÃ©curitÃ©. Cependant, cette annÃ©e, je pense quâ□□il est nÃ©cessaire de faire Ã©voluer certaines idÃ©es dÃ©passÃ©es en matiÃ¨re de cybersÃ©curitÃ©, et de mettre de cÃ´tÃ© les stÃ©rÃ©otypes usÃ©s jusquâ□□Ã la moelle ci-dessous

â□¢ Â« Il faut sensibiliser aux questions de cybersÃ©curitÃ© Â» â□□ La notion de cybersÃ©curitÃ© sâ□□est imposÃ©e au grand public lâ□□annÃ©e derniÃ¨re. Compte tenu du nombre dâ□□attaques

de ransomware lancÃ©es sur de grandes entreprises, des campagnes menÃ©es par des Ã□tats-nations et de lâ□□accent placÃ© par lâ□□administration amÃ©ricaine sur la cybersecuritÃ©, les gens sont clairement conscients du danger.

LÃ nâ□□est plus le problÃ¨me : le souci rÃ©side dans le fait que les individus sont lassÃ©s par la succession de compromissions faisant lâ□□actualitÃ©, et donnant la sensation dâ□□une situation dÃ©sespÃ©rÃ©e.

â□¢ Â« La sÃ©curitÃ© est lâ□□affaire de tous Â» â□□ Cela reste vrai Ã de nombreux Ã©gards. Chaque employÃ© doit Ãªtre vigilant et prendre une part active dans la sÃ©curitÃ© de son entreprise... cependant, nous nâ□□en faisons pas assez pour les aider Ã remettre leur rÃ´le en contexte.

La plupart des gens ne se considÃ¨rent pas comme des cibles, car ils ne pensent pas Ãªtre Â« dignes dâ□□intÃ©rÃªt Â», alors quâ□□en rÃ©alitÃ©, ils peuvent Ãªtre les intermÃ©diaires idÃ©aux vers une victime dÃ©signÃ©e. Nous avons Ã©galement besoin dâ□□individus dont lâ□□unique mission est la cybersÃ©curitÃ©.

La pÃ©nurie de compÃ©tences actuelle reprÃ©sente une menace existentielle. En 2022, les CEO et conseils dâ□□administration devraient donc en prioritÃ© chercher Ã recruter et fidÃ©liser autant de professionnels de la cybersÃ©curitÃ© que possible.

â□¢ Â« Lâ□□humain est le maillon faible Â» â□□ Les individus reprÃ©sentent des points dâ□□entrÃ©e pour les attaquants et commettent effectivement des erreurs (comme le fait de cliquer sur les liens dâ□□e-mails de phishing, ce qui reste malheureusement bien trop frÃ©quent). Pourtant, cet argument omet ou sous-estime les nombreuses faiblesses et vulnÃ©rabilitÃ©s des Ã©quipements et logiciels.

Combien de mises Ã jour de sÃ©curitÃ© Zoom ou Microsoft ont-ils dÃ» publier le mois dernier, par exemple ? La rÃ©ponse : Ã©normÃ©ment. Dans de nombreux cas, les employÃ©s restent les meilleurs atouts pour protÃ©ger leurs entreprises, donc mieux vaut ne pas les prÃ©senter comme Ã©tant plus faibles quâ□□ils ne le sont rÃ©ellement, ou les pointer du doigt. Soyons charitables et proposons-leur des formations en cybersÃ©curitÃ©, plutÃ´t que dâ□□ignorer les autres maillons faibles de la chaÃ®ne.

Le secteur hyper concurrentiel de la cybersÃ©curitÃ© se laisse souvent aller Ã des promesses quant Ã lâ□□existence de solutions magiques, capables Ã elles seules Â« sauver une organisation Â».

Les nouvelles technologies sont en effet essentielles Ã la cybersÃ©curitÃ©, et les Ã©diteurs font preuve dâ□□un sens de lâ□□innovation incroyable qui aide les entreprises Ã protÃ©ger leurs infrastructures, actifs, employÃ©s et clients. Mais nâ□□oublions pas quâ□□elles ne se suffisent pas Ã elles-mÃªmes. Lâ□□efficacitÃ© et la proactivitÃ© de la stratÃ©gie adoptÃ©e dÃ©pendront toujours des individus et des pratiques mises en Å□uvre.

Chris Hallenbeck, responsable de la sÃ©curitÃ© des systÃ¨mes dâ□□information, Tanium