Le SOC à l'épreuve du Covid-19

Si les employés ne peuvent pas interagir en personne avec leurs collègues, prendre un café avec eux ou sortir déjeuner, ils voient cependant leur attention détournée par des e-mails malveillants susceptibles d'exposer leur entreprise à des cyberattaques.

Les cybercriminels le savent très bien et profitent de ces nouveaux environnements de travail propices aux distractions pour lancer des cyberattaques.

Comme le rapporte Cisco Talos, bien que les auteurs des récentes attaques s'en tiennent à des techniques éprouvées comme le phishing, la fraude et les campagnes de désinformation, ils redoublent actuellement d'efforts et organisent leurs efforts autour du thème du Covid-19.

Depuis janvier, Barracuda Networks constate une augmentation régulière du nombre d'attaques de phishing liées au coronavirus. Parmi elles figurent un grand nombre d'arnaques à l'appel aux dons. D'autres concernent la vente de fournitures en lien avec la pandémie, comme de faux masques. Certains cybercriminels prétendent même agir au nom de services gouvernementaux pour aider les entreprises à faire face aux conséquences économiques de la crise. Leur principale motivation est l'appât du gain.
Toutefois, certaines attaques ont également pour but de distribuer des malwares aux télétravailleurs et d'infiltrer les réseaux d'entreprise.

Les dernières attaques majeures qui ont touché des secteurs d'activité, comme celui de la santé, ou des régions, comme Marseille et sa métropole révèlent que les attaques opportunistes sont inévitables. La situation actuelle est cependant différente. Il s'agit d'un phénomène mondial évolutif, dont il est difficile d'entrevoir la fin.

Une nouvelle réalité avec laquelle il va falloir composer encore longtemps. Les attaques se poursuivront et les employés baisseront de plus en plus la garde.

Les équipes de sécurité sont sur le pied de guerre et doivent protéger une infrastructure en mutation contre des cybercriminels à la recherche de cibles faciles. Le problème est qu'elles travaillent elles aussi à distance.

Les analystes du SOC et les membres de l'équipe de réponse aux incidents n'ont plus la possibilité de se réunir autour d'un bureau pour comparer les données et les analyses, ni de se rendre au bout du couloir pour discuter avec un analyste des renseignements sur les menaces.
Quant aux responsables des équipes de sécurité, difficile d'aller taper sur l'épaule d'un analyste pour lui confier une tâche ou lui demander l'état d'avancement d'une investigation.
Malgré les distances géographiques, les analystes et les responsables de la sécurité doivent être à même de collaborer efficacement avec les membres de l'équipe et entre les équipes.

Pour améliorer les opérations de sécurité dans un contexte de télétravail généralisé, les entreprises ont besoin d'un environnement collaboratif en ligne unique qui fusionne les données, les preuves et les utilisateurs.

Au cœur de ce système se trouve un référentiel central renfermant tous les renseignements de

l'entreprise sur les menaces mondiales, complétés et enrichis par des informations contextuelles internes sur les menaces et les événements.
Les différentes équipes de sécurité et chacun de leurs membres ont ainsi accès aux renseignements dont ils ont besoin pour accomplir leurs tâches respectives, et peuvent partager activement leurs connaissances ou communiquer directement entre eux.

Travailler dans la « salle de crise » virtuelle dédiée à la cybersécurité accélère leur compréhension des menaces et améliore la collaboration. Si les incidents se multiplient en raison d'une intensification des campagnes de cyberattaques, il leur est possible de se répartir les tâches afin de se concentrer sur le blocage et la neutralisation.
Au lieu de mener des investigations en parallèle, tous les membres d'équipe impliqués dans le processus d'investigation peuvent automatiquement voir le travail des autres, et comprendre son incidence et ses effets positifs sur leur propre travail.

Cet environnement collaboratif présente aussi des avantages pour les responsables des équipes de sécurité. Il leur permet de superviser les investigations à distance en observant le déroulement de l'analyse, et en pilotant les opérations de manière opportune et adéquate.
Ils peuvent décomposer les tâches et les affecter à des intervenants spécifiques d'une simple « tape virtuelle sur l'épaule », coordonner les tâches entre les équipes, et surveiller les échéances et les résultats.

Grâce à la collaboration en ligne intégrée aux opérations de sécurité, les responsables s'assurent que les analystes de la sécurité, où qu'ils se trouvent physiquement, sont en mesure de travailler efficacement ensemble afin d'accélérer la détection et la réponse.

En cette période où les cybercriminels, en quête de proies faciles, n'hésitent pas à exploiter les faiblesses potentielles de notre nouvelle normalité, une salle de crise virtuelle dédiée à la cybersécurité permet aux équipes de travailler de concert en s'appuyant sur des données pertinentes pour prendre de bonnes décisions plus rapidement et renforcer la sécurité.
Même si leurs analystes travaillent depuis leur domicile, les responsables de la sécurité peuvent continuer à coordonner les investigations et les mesures correctives.

Chacun s'accorde à reconnaître que la pandémie mondiale aura des effets durables sur nos modes de vie actuels. Alors que nous cherchons un rayon d'espoir, la salle de crise virtuelle dédiée à la cybersécurité est un modèle dont nous avons plus que jamais besoin et, surtout, qui restera un sérieux atout pour les professionnels de la sécurité même lorsque la vie reprendra son cours « normal »