Mettre en Å□uvre un programme de gestion continue de l'exposition aux menaces
Internet
PostÃ© par : JulieM
PubliÃ©e le : 13/3/2023 13:00:00

Selon certains cabinets dâ□□analyse stratÃ©gique Â« Les entreprises Ã©chouent Ã rÃ©duire leur exposition aux menaces car elles tentent dâ□□Ã©valuer le risque via des outils disparates et non normalisÃ©s.

De plus, des mÃ©thodes de traitement obsolÃ¨tes ne permettent pas de vaincre les silos organisationnels Â», dixit Sylvain CORTES chez Hackuity

Lâ□□annÃ©e 2023 doit Ãªtre celle du changement de paradigme, les responsables sÃ©curitÃ© ainsi que les gestionnaires de risques doivent lancer et faire Ã©voluer un programme de gestion continue de l'exposition aux menaces afin de garder une longueur d'avance et Ãªtre en capacitÃ© dâ□□Ã©valuer et corriger les vulnÃ©rabilitÃ©s critiques prÃ©sentes dans lâ□□organisation.

Un programme de gestion continu de lâ□□exposition aux menaces repose sur un cycle rÃ©pÃ©titif constituÃ© de cinq Ã©tapes principales :

Cadrage

Il est important de dÃ©finir le pÃ©rimÃ¨tre du programme afin de consacrer les efforts sur les Ã©lÃ©ments stratÃ©giques pour le business. Au fur et Ã mesure de lâ□□Ã©volution des systÃ¨mes IT internes ou externes il est tout Ã fait possible de modifier ce cadrage Ã chaque itÃ©ration du cycle.

Si bien sur lâ□□IT historique et hÃ©bergÃ© au sein de lâ□□organisation fait toujours parti de ce type de cadrage, il sera important de penser Ã rajouter d'autres pÃ©rimÃ¨tres impliquant un risque non nÃ©gligeable pour le business : Attaque de la surface externe, sÃ©curitÃ© des donnÃ©es dans les applications SaaS, dÃ©pÃ´ts du code des applications business, etc. Cette Ã©tape souvent nÃ©gligÃ©e reprÃ©sente pourtant le fondement de tout le cycle.

DÃ©couverte

Malheureusement, beaucoup de praticiens confondent encore lâ□□Ã©tape de cadrage de celle de dÃ©couverte et imaginent quâ□□il suffit de dÃ©couvrir des Ã©lÃ©ments pour assurer le succÃ¨s du cycle. Les outils de dÃ©couverte doivent prendre en compte de nombreux aspects afin dâ□□identifier les diffÃ©rents types de vulnÃ©rabilitÃ©s, quâ□□elles soient liÃ©es Ã du code ou Ã des erreurs de configuration.

Priorisation

L'objectif du cycle n'est pas d'essayer de remÃ©dier Ã tous les problÃ¨mes identifiÃ©s car cela est impossible, il sâ□□agit plutÃ´t dâ□□Ã©valuer et de traiter les menaces les plus susceptibles d'Ãªtre exploitÃ©es contre l'organisation. Les organisations ne peuvent pas utiliser les mÃ©thodes traditionnelles de hiÃ©rarchisation des expositions via des scores de gravitÃ© de base prÃ©dÃ©finis.

La priorisation du traitement des expositions doit Ãªtre basÃ©e sur une combinaison des Ã©lÃ©ments suivants : existence ou non des exploits liÃ©s Ã la vulnÃ©rabilitÃ©, les options

d'attÃ©nuation de la menace prÃ©sentes sur le systÃ¨me, le niveau dâ□□exposition et dâ□□atteinte du dit systÃ¨me, la criticitÃ© de l'activitÃ© portÃ©e par les systÃ¨mes, etc.

Validation

Lâ□□Ã©tape de validation consiste Ã atteindre principalement deux objectifs : Ã□valuer la probabilitÃ© pour que lâ□□exÃ©cution dâ□□une attaque soit rÃ©ussie en confirmant notamment que les attaquants pourraient rÃ©ellement exploiter les expositions prÃ©cÃ©demment dÃ©couvertes -

Estimer l'impact potentiel le plus Ã©levÃ© en pivotant au-delÃ de l'empreinte initiale et en analysant tous les chemins d'attaque potentiels vers un actif critique depuis la compromission initiale. La pratique utilise une combinaison dâ□□outils et dâ□□activitÃ©s tels que le pentesting, les activitÃ©s de red team, la simulation de brÃ¨che et d'attaque, etc.

Mobilisation

AprÃ¨s validation de la liste des vulnÃ©rabilitÃ©s prioritaires Ã corriger, la remÃ©diation ne peut pas Ãªtre entiÃ¨rement automatisÃ©e, de nombreuses organisations matures ont atteint les limites de la "remÃ©diation automatisÃ©e" car les traitements techniques nÃ©cessitent trÃ¨s souvent l'application de correctifs ou la rÃ©alisation d'un changement de configuration.

Il est donc nÃ©cessaire de coupler les mÃ©thodes pleinement automatisÃ©es aux traitement basÃ©s sur un systÃ¨me de tickets et de workflows.