CybercriminalitÃ© : le manque de confiance pÃ©nalise.
Internet
PostÃ© par : JulieM
PubliÃ©e le : 22/4/2022 15:00:00

PrÃ¨s dâ□□un tiers (27 %) des responsables IT franÃ§ais manquent de confiance dans leur capacitÃ© Ã combler leurs lacunes en matiÃ¨re de sÃ©curitÃ©, selon une enquÃªte HackerOne

Le concept de â□□dÃ©ficit de rÃ©sistance aux attaquesâ□□ sâ□□explique par une connaissance incomplÃ¨te des surfaces d'attaque, des tests de sÃ©curitÃ© trop peu frÃ©quents, des outils de test peu sophistiquÃ©s et un manque de compÃ©tences techniques.

HackerOne, le leader mondial du hacking Ã©thique, dÃ©voile aujourdâ□□hui le rapport The 2022 Attack Resistance, qui recueille les Ã©valuations des professionnels de lâ□□IT sur leur Ã©tat de prÃ©paration contre des cyberattaques.

Ce rapport rÃ©vÃ¨le que les organisations sont confrontÃ©es Ã un Ã©cart important entre ce qu'elles doivent protÃ©ger et ce quâ□□elles sont rÃ©ellement capables de protÃ©ger - Cet Ã©cart est appelÃ© "dÃ©ficit de rÃ©sistance aux attaques".

ConnaÃ®tre sa surface dâ□□attaque nâ□□est pas suffisant

Le rapport The 2022 Attack Resistance sâ□□appuie sur les rÃ©sultats dâ□□une enquÃªte rÃ©alisÃ©e auprÃ¨s de 800 organisations en France, au Royaume-Uni, en Allemagne et en AmÃ©rique du Nord. Il examine quatre domaines essentiels permettant aux organisations dâ□□Ã©valuer et dâ□□amÃ©liorer leur rÃ©sistance aux cyberattaques :

1. La comprÃ©hension de la surface d'attaque.
2. La cadence des tests par rapport aux cycles de lancement des applications.
3. Le type et la frÃ©quence des tests de sÃ©curitÃ©.
4. La disponibilitÃ© de talents techniques capables de bien mener ces tÃ¢ches.

En mesurant le niveau de confiance des organisations sur lâ□□ensemble de ces quatre domaines, il apparaÃ®t que la France est le pays qui a le score de confiance le plus faible dans sa rÃ©sistance aux cyberattaques (59 %), en dessous du score de confiance moyen qui sâ□□Ã©tablit Ã 63 %.

Voici les principales conclusions de cette enquÃªte :

â□¢ Combler le dÃ©ficit de rÃ©sistance aux attaques est un vÃ©ritable dÃ©fi en France : 27 % des organisations franÃ§aises manquent de confiance dans leur capacitÃ© Ã rÃ©duire leur dÃ©ficit de rÃ©sistance aux attaques (15 % en Allemagne, 17 % au Royaume-Uni, 18 % aux Ã□tats-Unis).

â□¢ Les surfaces dâ□□attaques ne sont pas suffisamment surveillÃ©es : 60 % des organisations interrogÃ©es avouent quâ□□un quart de leur surface dâ□□attaque est inconnue ou non observable, ce qui les rend vulnÃ©rables aux menaces externes dans le contexte oÃ¹ la transformation numÃ©rique sâ□□accÃ©lÃ¨re.

En France, 12% des responsables interrogÃ©s estiment que plus de la moitiÃ© de leur surface d'attaque est inconnue ou non observable. Les organisations franÃ§aises sont Ã©galement celles qui scannent le moins frÃ©quemment leur surface dâ□□attaque - 29 % des responsables IT

franÃ§ais interrogÃ©s scannent leur surface dâ□□attaque une fois par mois ou encore moins souvent, lÃ oÃ¹ la plupart des organisations des autres rÃ©gions observÃ©es le font quotidiennement (35 % au Royaume-Uni, 38 % aux Ã□tats-Unis, 41 % en Allemagne et seulement 21 % en France).

â□¢ La pÃ©nurie de talents techniques diminue la capacitÃ© des organisations Ã protÃ©ger leur surface d'attaque. La France est le pays qui exprime le plus dâ□□inquiÃ©tudes Ã ce sujet. 58 % des responsables IT franÃ§ais peinent Ã trouver des collaborateurs qui maÃ®trisent la complexitÃ© des environnements cloud (contre 53 % au Royaume-Uni, 52 % aux Ã□tats-Unis, 43 % en Allemagne) et 63 % rÃ©vÃ¨lent que le manque de profils techniques Ã lâ□□embauche les pousse Ã externaliser leur sÃ©curitÃ© (contre 59 % au Royaume-Uni, 55 % aux Ã□tats-Unis et 46 % en Allemagne).

â□¢ Lâ□□insuffisance de tests ajoute une pression supplÃ©mentaire. 39 % des organisations franÃ§aises rÃ©alisent moins de 100 tests de pÃ©nÃ©tration par an (contre 29 % au Royaume-Uni, 27 % aux Ã□tats-Unis et 26 % en Allemagne) et 44 % rÃ©alisent moins de 100 Ã©valuations de sÃ©curitÃ© par an (contre 40 % au Royaume-Uni, 29 % aux Ã□tats-Unis et 43 % en Allemagne).

â□¢ Les outils de gestion de surface dâ□□attaque (ASM - Attack Surface Management) sont davantage perÃ§us comme une obligation quâ□□un outil stratÃ©gique pour amÃ©liorer la posture globale de sÃ©curitÃ©. Se mettre en conformitÃ© avec le RGPD est par exemple la principale raison dâ□□utiliser des outils de gestion de surface dâ□□attaque pour 50 % des responsables IT franÃ§ais interrogÃ©s.

â□□La prise de conscience rÃ©duit le risque. Seules les organisations qui mesurent leur dÃ©ficit de rÃ©sistance aux attaques sont armÃ©es pour le rÃ©duireâ□□, a dÃ©clarÃ© Marten Mickos, PDG de HackerOne. â□□Nous avons menÃ© cette enquÃªte pour illustrer le phÃ©nomÃ¨ne et donner des pistes dâ□□amÃ©lioration. Les organisations qui Ã©largissent le cadre de leurs tests, et qui le font de maniÃ¨re continue peuvent combler ce dÃ©ficit de rÃ©sistance aux attaques.â□□

Consultez le rapport.