CybersÃ©curitÃ© : EnquÃªte exclusive au sein des entreprises franÃ§aises
Internet
PostÃ© par : JPilo
PubliÃ©e le : 1/2/2023 14:00:00

Afin de mieux cerner lâ□□Ã©tat de lâ□□art et la perception de la cybersÃ©curitÃ© et de ses enjeux au sein des entreprises franÃ§aises, le CESIN publie depuis 2015 son baromÃ¨tre annuel avec OpinionWay.

Lâ□□association dÃ©voile aujourdâ□□hui les rÃ©sultats de cette nouvelle enquÃªte indÃ©pendante et exclusive menÃ©e auprÃ¨s de ses membres, Directeurs CybersÃ©curitÃ© et Responsables SÃ©curitÃ© des SystÃ¨mes d'Information (RSSI) des entreprises franÃ§aises. Ce sondage OpinionWay pour le CESIN porte sur un Ã©chantillon de 328 rÃ©pondants, membres du CESIN.

Lâ□□Ã©tude rÃ©vÃ¨le que les cyberattaques sont en baisse. Elles concernent dÃ©sormais moins dâ□□une entreprise sondÃ©e sur deux. (le baromÃ¨tre tient compte uniquement des attaques rÃ©ussies, ayant eu des rÃ©percussions significatives pour les victimes - cf : dÃ©finition de Cyberattaque pour lâ□□enquÃªte CESIN-OpinionWay 1).

La menace est toujours trÃ¨s prÃ©sente, nÃ©anmoins lâ□□anticipation semble porter ses fruits Ã mesure des politiques de sensibilisation, de lâ□□investissement dans les outils de protection, de la capacitÃ© de dÃ©tection et de gestion des incidents, ou de lâ□□entraÃ®nement aux situations de crises.

Les attaques par ransomware ont touchÃ© moins dâ□□1 entreprise sur 5. Cependant, si pour 64% des rÃ©pondants le nombre dâ□□attaques abouties est restÃ© stable, cela ne signifie pas que lâ□□activitÃ© soit moins dense, 24% des entreprises ayant dÃ©clarÃ© au moins une attaque en 2022 estiment toujours que le phÃ©nomÃ¨ne est en augmentation.

Le Phishing reste le vecteur dâ□□attaque le plus frÃ©quent. 74% des entreprises dÃ©clarent le Phishing comme vecteur dâ□□entrÃ©e principal pour les attaques subies.

Parmi les autres moyens de transmission, en tÃªte du classement lâ□□exploitation des failles (45%) et nous savons que le nombre de vulnÃ©rabilitÃ©s, mais aussi la surface dâ□□attaque publique sont en constante augmentation, ou encore lâ□□attaque par rebond via un prestataire (24%). Sur ce point, notons que la gestion des risques liÃ©s aux tiers prend une place de plus en plus importante dans les activitÃ©s des responsables cybersÃ©curitÃ©.

Dans 60% des cas, les attaques impactent fortement le business des entreprises, avec pour effet de perturber significativement la production pour 24% des sondÃ©s. Dans 7% des cas on constate un dÃ©ficit du chiffre dâ□□affaires. Au nombre des prÃ©judices, le vol de donnÃ©es (35%), lâ□□usurpation dâ□□identitÃ©s (33%), et les donnÃ©es chiffrÃ©es par ransomware (22%).

Plus dâ□□une entreprise sur deux considÃ¨re toujours que le niveau de menaces en matiÃ¨re de cyberespionnage est Ã©levÃ© (50%). Ces opÃ©rations visent le plus souvent des cibles dâ□□intÃ©rÃªts stratÃ©giques.

Une dynamique Ã nouveau confirmÃ©e par lâ□□Agence nationale de la sÃ©curitÃ© des systÃ¨mes dâ□□information (ANSSI), qui rappelle que le ciblage des victimes peut affecter les fournisseurs dâ□□opÃ©rateurs stratÃ©giques, leurs prestataires et parfois leurs autoritÃ©s de tutelle.

A propos du Cloud, qui reprÃ©sente moins de 50% du SI en moyenne chez les rÃ©pondants, les principaux facteurs de risques induits concernent toujours la non maÃ®trise de la chaÃ®ne de sous-traitance de lâ□□hÃ©bergeur et la difficultÃ© de contrÃ´le des accÃ¨s par les administrateurs de lâ□□hÃ©bergeur.

La surveillance de la sÃ©curitÃ© des clouds requiert des outils spÃ©cifiques et dans la grande majoritÃ© des cas (89%) il est jugÃ© nÃ©cessaire dâ□□utiliser dâ□□autres dispositifs que ceux proposÃ©s nativement par les fournisseurs de cloud.

6 entreprises sur 10 se disent prÃ©occupÃ©es par les sujets de souverainetÃ© et de cloud de confiance. Ce qui suppose toujours une attente forte autour des perspectives de potentiels rÃ©Ã©quilibrage des forces avec le dÃ©veloppement de solutions dites de confiance annoncÃ©es en France et en Europe.

Lâ□□axe sensibilisation est au rang des mesures qui progressent pour faire face aux dÃ©fis de la cyber. 8 entreprises sur 10 mÃ¨nent des campagnes de sensibilisation auprÃ¨s des collaborateurs.

La culture de la cybersÃ©curitÃ© nâ□□est pourtant toujours pas suffisamment ancrÃ©e dans les organisations, seuls 2/3 des utilisateurs respectent les recommandations. Dâ□□autant que la nÃ©gligence et les erreurs de manipulation constituent la principale cause dâ□□incidents (38%).

Alors que tous les collaborateurs ont un rÃ´le Ã jouer en matiÃ¨re de cybersÃ©curitÃ©, on dÃ©plore encore un manque dâ□□expertise sÃ©curitÃ© pour les administrateurs, architectes ou dÃ©veloppeurs, une compÃ©tence qui permettrait un progrÃ¨s significatif dans la contribution de chacun de ces mÃ©tiers Ã rÃ©duire les risques.

Les outils sont au cÅ□ur de la politique de protection avec une moyenne dâ□□adoption de 15 solutions et services par organisation. On constate un bon niveau de confiance dans les solutions puisque 88% des rÃ©pondants jugent les solutions du marchÃ© plutÃ´t adaptÃ©es.

Une place prÃ©pondÃ©rante est donnÃ©e aux outils de dÃ©tection et de rÃ©ponse aux incidents. Lâ□□authentification multi-facteurs concerne 81% des entreprises et est rÃ©putÃ©e performante. Câ□□est dâ□□autant plus important que 33% des attaques ont conduit Ã des usurpations dâ□□identitÃ©s.

On note une forte hausse du dÃ©ploiement des EDR, devenu une rÃ©alitÃ© dans 81% des entreprises. Les outils de gestion des vulnÃ©rabilitÃ©s ainsi que les services de SOC comptent parmi les dispositifs jugÃ©s les plus efficaces. Enfin, on peut noter que 6 entreprises sur 10 ont recours Ã des offres innovantes issues de start-up.

Les budgets allouÃ©s Ã la cybersÃ©curitÃ© augmentent encore lÃ©gÃ¨rement cette annÃ©e. Ils dÃ©passent majoritairement 5% du budget IT global. 63% prÃ©voient une augmentation allouÃ©e aux dispositifs de protection, et 54% attribuÃ©e Ã lâ□□augmentation des effectifs.

82% prÃ©voient dâ□□acquÃ©rir de nouvelles solutions. In fine 77% estiment avoir les moyens de se prÃ©munir dâ□□une cyberattaque de grande ampleur, mais plus de la moitiÃ© se dÃ©clare limitÃ©e dans son aptitude Ã rÃ©pondre et reconstruire. La rÃ©silience des SI face Ã des cyberattaques reste un maillon important Ã amÃ©liorer dans la stratÃ©gie de dÃ©fense.

PrÃ¨s de 2/3 des rÃ©pondants ont souscrit une cyberassurance. Les premiers bilans rÃ©vÃ©laient un moindre taux de satisfaction pour ceux qui avaient eu recours Ã lâ□□assurance, tandis que 76% dâ□□entre elles ne lâ□□ont pas utilisÃ©e.

Cette annÃ©e, 1 rÃ©pondant sur 10 se dÃ©clare hÃ©sitant pour renouveler son contrat, et 2% y ont dÃ©jÃ renoncÃ©. En outre, une majoritÃ© dâ□□entreprises Ã©met un avis nÃ©gatif sur le

recours aux services dâagences de notation par les assureurs.

De son cÃ´tÃ© Le CESIN note toujours une forte hausse des tarifs, pour une baisse des couvertures, avec toujours plus dâexclusions, et des niveaux dâexigences de la part des assureurs, quasiment inatteignables.

En parallÃ¨le la prise en compte des enjeux de cybersÃ©curitÃ© au sein du COMEX est stable. Le sujet cybersÃ©curitÃ© est bien prÃ©sent dans les COMEX. 75% des rÃ©pondants sont confiants sur lâengagement de leur comitÃ© exÃ©cutif. Placer la gouvernance de la cybersÃ©curitÃ© au bon niveau dans lâentreprise est au premier rang des objectifs dâavenir.Â