Mardi 11 juillet 2023

Communiqué de presse

Premier baromètre cyber breton: la Région Bretagne prend le pouls de ses acteurs économiques en cybersécurité.

Selon une étude réalisée par Bretagne Développement Innovation pour le compte de la Région Bretagne auprès de 269 organisations régionales (entreprises, collectivités, associations), 36% des acteurs déclarent avoir subi un incident de sécurité informatique ; la plupart du temps par rançongiciel. 52% des répondants de l'enquête déclarent qu'ils seraient en incapacité de délivrer leurs services sans système d'information, d'où l'intérêt d'observer et de suivre leur degré de maturité et leur connaissance en matière de cybersécurité. Si la majorité des organisations ont déjà mis en place un premier niveau de protection (antivirus, pare-feu périmétrique…), il reste cependant une belle marge de progression au regard de la menace croissante de cyberattaques. En partant des pratiques et des besoins du terrain, ce baromètre compile des données concrètes. Ces informations seront précieuses à l'EDIH Bretagne (le « European Hub » de la région Bretagne pour booster l'innovation numérique ainsi qu'au futur CSIRT régional pour accompagner les organisations régionales à se protéger efficacement.

Région pionnière et porteuse en matière de cybersécurité en France et en Europe, la Bretagne se dote désormais d'un baromètre évaluant le degré de maturité et les besoins en cybersécurité de ses organisations publiques et privées.

Cet outil est le fruit d'une étude menée entre mars et mai 2023 auprès de 269 acteurs implantés en Bretagne :

- 45% de collectivités locales
- 50% d'entreprises
- 5% d'associations

Guillaume Chéreau, responsable du CSIRT Bretagne au sein de la Région Bretagne explique : "*L'objectif de cette étude était de savoir comment les organisations bretonnes perçoivent les risques, quel est leur niveau de maturité quant aux questions de cybersécurité, ce qu'elles mettent déjà en œuvre, la connaissance des dispositifs d'accompagnement, leurs besoins et les éventuels freins à la mise en œuvre d'une politique spécifique à la cybersécurité.* "

Un tiers des organisations bretonnes déjà victimes d'une cyberattaque

Le baromètre cyber breton révèle que plus d'un tiers des organisations répondantes (36%) a déjà subi une cyberattaque. "*Dans 45% des cas, le mode opératoire était un rançongiciel. La fraude par ingénierie sociale (technique de manipulation utilisée par les cybercriminels pour inciter les gens à partager des informations confidentielles par exemple) représente 26% des attaques",* précise Guillaume Chéreau.

Un niveau minimal d'hygiène informatique…

Le baromètre dresse un état des lieux de l'implémentation des mesures cyber d'hygiène fondamentales. Ainsi, 92% des entités ont mis en place une politique de protection par antivirus, 76% un système de protection de la messagerie et 84% une solution de pare-feu périmétrique. "*Les chiffres démontrent que la très grande majorité des entités bretonnes, qu'elles soient publiques ou privées, ont le niveau minimal en matière d'hygiène informatique,"* poursuit Guillaume Chéreau. En revanche, on note une faiblesse sur la mise à jour des serveurs parmi les solutions déployées avec seulement 51% des répondants.

… mais des mesures avancées encore faibles

Les organisations bretonnes ont une large marge de progression lorsqu'il s'agit d'instaurer des stratégies de protection et de prévention plus avancées recommandées par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). Hormis pour les sauvegardes hors-ligne (sur disques durs externes ou des bandes dédiées), qui sont mises en place au sein de 73% des entités répondantes, les autres mesures prioritaires ne sont pas assez mises en place, avec un niveau moyen d'implémentation de l'ordre de 40%. Dans le détail :

- Dispositif de gestion de crise adapté à une cyberattaque : 40%
- Liste priorisée des services numériques critiques de l'entité : 37%
- Supervision de sécurité : 23%
- Authentification multifacteurs : 32%

*"Le faible taux de réponses positives pour l'authentification multi-facteurs et la supervision représente un point noir important, s*ouligne Guillaume Chéreau. *Aujourd'hui, les ordinateurs compromis par des maliciels dérobeurs, des infostealers, se comptent par milliers, à travers le monde, chaque jour. L'authentification multi-facteurs s'avère indispensable pour contrer ce phénomène rendant accessible des identifiants, parfois professionnels, aux cybercriminels. Concernant la supervision, aujourd'hui, il ne faut plus se contenter d'une protection périmétrique. Ce sont deux axes de progrès majeurs."*

Moyens et politiques de cybersécurité

En moyenne, les répondants consacrent 6,5% de leur budget informatique à la cybersécurité. Une part importante des répondants (36%) déclare ne pas avoir connaissance du budget cybersécurité.

Côté organisation, 88% des répondants déclarent qu'aucun processus de gouvernance de la sécurité n'est mis en œuvre dans leur organisation.

En matière de formation, 87% des répondants déclarent avoir réalisé des sessions de sensibilisation à l'attention de leurs collaborateurs et 61% des dirigeants des organisations ont été sensibilisés.

Le manque de ressources humaines est souvent cité comme principal frein aux politiques de sécurité (61 % des répondants). Les moyens financiers (40%) et le manque de compétences au sein des équipes informatiques (29%), complètent ce triptyque. Le manque d'intérêt et des priorités autres sont très peu caractérisés parmi les répondants, démontrant ainsi une vraie prise en compte du risque cyber.

Une base de travail pour l'EDIH Bretagne et le futur CSIRT

Le baromètre cyber, en dressant un état des lieux de la maturité des organisations bretonnes, fournit mine d'informations à l'EDIH Bretagne et au futur CSIRT-Bretagne (centre de réponse à incidents cyber). Les entreprises, collectivités et associations pourront se tourner vers ces deux outils régionaux pour trouver des solutions et répondre aux normes de cybersécurité exigées. "*Les résultats de l'enquête montrent que ces deux outils ont une véritable raison d'être et sont complémentaires. L'EDIH,*

afin d'accompagner la transformation numérique, avec la mise en place d'un niveau de sécurité qui monte aussi vite que la numérisation. Les entités répondantes ont pu faire part de leur intérêt pour être mises en relation avec l'EDIH. Le CSIRT, qui est en cours d'incubation, apportera des services autour de la réponse à incidents."

>> Découvrir l'intégralité des résultats de l'enquête :

https://www.calameo.com/read/0050832086fe0c31d3e53

A propos du baromètre cyber breton

Le baromètre cyber breton a été réalisé en partenariat avec le syndicat mixte Megalis, le CLUSIR, le club des ETI Bretagne et l'Ordre des experts comptables et supervisée par BDI pour le compte de la Région Bretagne. L'étude vient compléter l'annuaire des acteurs de la cybersécurité conçu par BDI.

L'enquête a été envoyée à 2 000 entités, 409 réponses ont été réceptionnées et 269 réponses complètes ont été traitées.

Contacts presse :
Bretagne Développement Innovation
Chrystèle Guy - 07 82 21 81 35 – c.guy@bdi.fr
Espace presse : https://www.bdi.fr/fr/presse/

Agence Oxygen
Emmanuelle Catheline - 06 79 06 36 11 - emmanuelle.c@oxygen-rp.com
Christelle Roignant - 06 83 81 61 61 - christelle@oxygen-rp.com