BAROMÈTRE DSI 2023

Une approche globale pour la cybersécurité

la clé pour vous protéger

Insight

Symantec by Broadcom

01

Introduction

Le sujet de la cybersécurité fait fréquemment l'objet de l'actualité médiatique. Mais, **quel est le vécu réel des organisations** ? A quel point sont-elles touchées et comment se protègent-elles ?

Nous avons questionné avec ce **nouveau Baromètre des DSI 2023** plus d'une centaine de directeurs informatiques et responsables de la sécurité informatique de grandes entreprises et d'administrations en France. Ils nous ont bien confirmé la persistance et même **une recrudescence des attaques en 2023**.

Ainsi, au cours des 6 derniers mois, 22% d'entre eux ont constaté un accroissement net des cyberattaques à leur encontre *(voir schéma 01 sur la page 3)*.

Sommaire

Il faut dire que **les brèches et médias par lesquels les cybercriminels peuvent attaquer un système sont nombreux**.

Citons notamment le site web, les serveurs, la plateforme d'e-commerce, les messageries ou le comportement du personnel sur site ou à distance *(voir schéma 05 sur la page 7)*.

Pour anticiper et éviter ces attaques touchant leurs infrastructures informatiques, nous nous sommes interrogés sur **la stratégie globale des grandes organisations** (entreprises et administrations) pour y faire face.

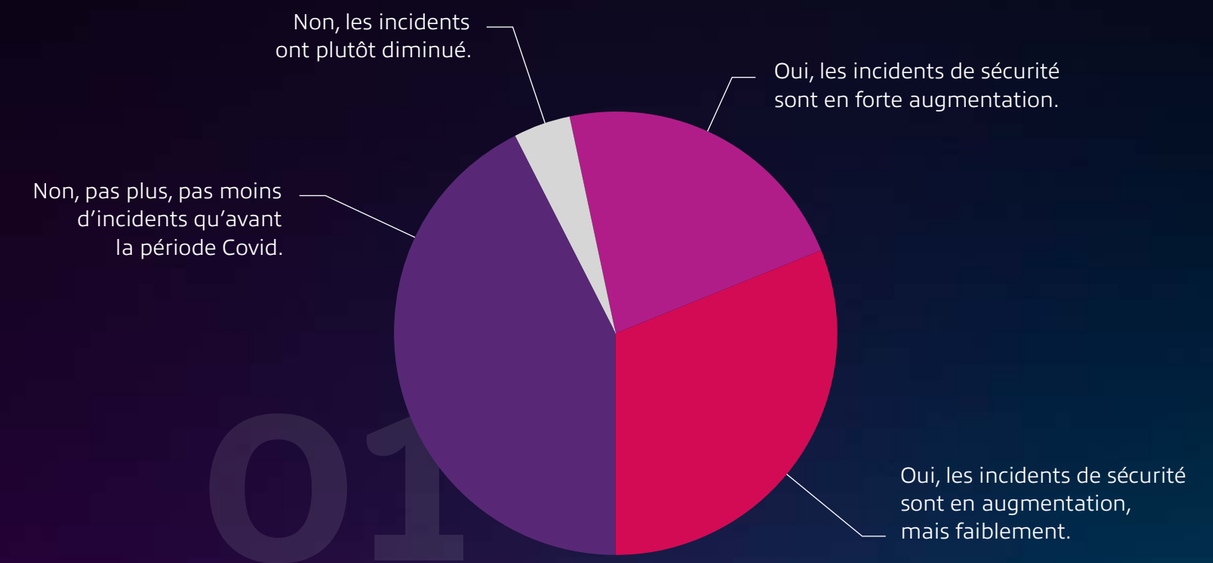
Quelles politiques de sécurité et quelles actions ont-elles mis en place pour empêcher ces actes de cybercriminalité ?

Pour répondre à cette question et bien d'autres encore, **une étude d'impact** a été réalisée pour le compte d'Insight et le support de Symantec Broadcom.

Une vingtaine de questions ont été posées à plus d'une centaine de DSI et RSSI dont 2/3 appartiennent au secteur privé et 1/3 au secteur public.

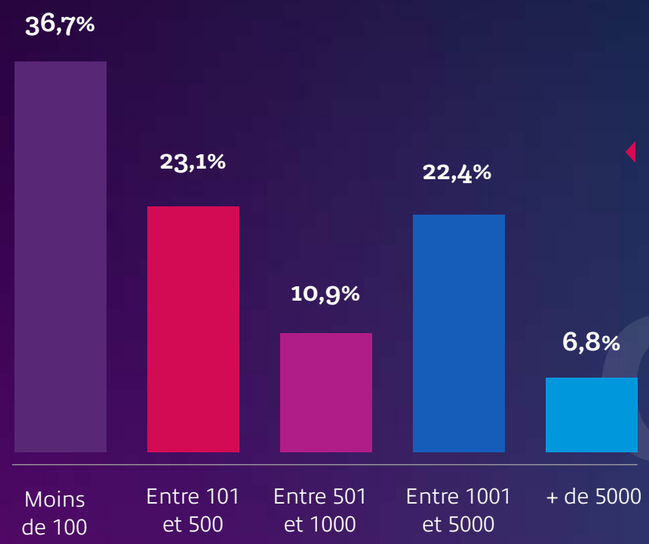
En analysant des données obtenues auprès d'ETI et d'organisations de plus de 500 personnes *(voir schéma 02)*, nous avons pu établir ce **baromètre sur l'état de la cybersécurité en 2023** en France.

Avez-vous constaté une augmentation des incidents de sécurité au 1er semestre 2023 ?



01

Quel est l'effectif de votre entreprise ?



02

02

La cybersécurité, une question stratégique au cœur de votre organisation

Avec l'accroissement des cyberattaques, la majorité de nos répondants ont mis en place des **parades et des politiques de prévention**. Et pour cause : la sécurité des systèmes informatiques est au cœur de la vie de leur organisation.

D'ailleurs, ce sont principalement des responsables opérationnels qui nous ont répondu, démontrant ainsi à quel point **l'enjeu d'une lutte efficace contre la cybercriminalité est stratégique**. Tous sont conscients du fait que **les cyberattaques mettent en péril leur organisation** allant des pertes financières à l'arrêt complet de leur activité.

D'après les chiffres du portail de l'IE[1], **le coût d'une attaque peut s'élever entre 15.000 euros et 4 millions d'euros** pour une entreprise.

[1] *Portail de l'Intelligence Économique*

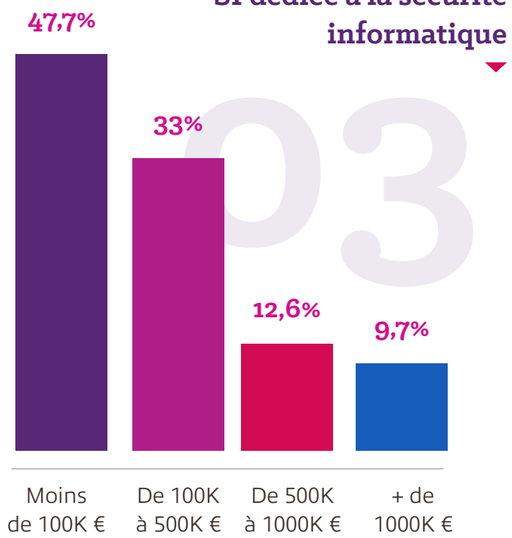
Dans ce contexte, on comprend que les budgets alloués à la sécurisation des systèmes informatiques ne sont pas des moindres.

> ***Ainsi, 2 DSI sur 10 dédient des budgets opérationnels de plus de 500.000€ par an pour contrer les attaques*** *(voir schéma 03).*

Bien que des ressources importantes soient dédiées à la cybersécurité, 1/3 des répondants estiment cependant ne pas être suffisamment protégés.

Fourchette de budget SI dédiée à la sécurité informatique

03



03

LES CYBERATTAQUES : de multiples formes et en augmentation

Obtenir un nombre précis de cyberattaques en France n'est pas aisé. De fait, **peu d'entreprises ou organisations osent répondre sincèrement** à la question de la fréquence des cyberattaques.

Référons-nous alors au rapport d'activité 2022 de la plateforme Cybermalveillance.gouv.fr[1] et ce chiffre de plus de 280.000 demandes d'assistance en un an.

Penchons-nous sur la notion de cyberattaque. Qu'englobe-t-elle ?

[1] *Cybermalveillance.gouv.fr*

> ***Il existe au moins 10 formes d'attaque possibles, soit autant de sources de faiblesses d'un système informatique***

- Attaques ransomware
- Phishing / Social Engineering
- Emails ave pièces jointes et scripts tiers
- Usurpations d'identité
- Déni de service - DDoS
- Piratage de site web / application
- Brèche de l'Active Directory
- Attaques à base d'IA
- Zéro Day Attack
- Interception de Traffic / «man in the middle»

Notre échantillon constitué de grandes entreprises et organisations cite le plus souvent ces **3 sources** :

- ***Le ransomware***
- ***Le phishing***
- ***Les pièces jointes*** dans un e-mail

Quant à la fréquence du phénomène, notre enquête nous montre qu'un DSI sur deux a constaté au moins **une de ces formes d'attaques au cours des 6 derniers mois** *(voir schéma 01 sur la page 3)*.

04

Face aux conséquences coûteuses, une volonté d'agir

Les conséquences d'une cyberattaque se chiffrent en dizaines voire centaines de milliers d'euros. On aurait tendance à penser, en premier lieu, aux phénomènes d'usurpation d'identité ou de demande de rançon, dont les effets directs prennent la forme de sorties d'argent. Mais, **une attaque peut également avoir des conséquences dont l'impact financier sera indirect** ou à effet retard.

Ainsi, une interruption de service peut entraîner des répercussions financières liées au temps nécessaire au rétablissement du service ou au temps perdu par les employés et les clients. Relevons que parmi nos répondants :

> ***Près d'une organisation sur 10, ont admis subir une interruption de service pendant plus de 24 heures.***

Et, une question additionnelle se pose : comment chiffrer les conséquences d'un vol de données ? Outre les fraudes en cascade que peuvent faire subir les cybercriminels aux personnes dont les données ont été volées (chantage, fraudes bancaires…), l'entreprise dont les données ont fuité verra sa réputation ternie voire sera sanctionnée pour non-conformité au RGPD !

Face à l'exposition de plus en plus fréquente de telles attaques, nous constatons que près d'une organisation sur deux (49,7%) affirme **une volonté de passer à l'action**, à commencer par la recherche des solutions de détection et de prévention, et ce dans les 6 prochains mois *(voir liste 04 et la schéma 06 sur la page 8)*.

L'importance et l'urgence d'agir font donc bien partie intégrante des préoccupations à court terme de nos répondants.

Projets d'amélioration en sécurité et protection IT

Détection / prévention des attaques	49,7%
Console de sécurité et de pilotage centralisé	35,9%
Protection des postes de travail, mobiles ou serveurs	31,1%
Gestion de vulnérabilité/Mise à jour du SI	30,1%
Accès à distance aux applications	26,2%
Flux réseaux	24,3%
Mise en conformité (SOC, ISO 2700, RGPD)	23,3%
Implémentation d'outils EDR OU XDR	19,4%
Implémentation étendue du Zéro Trust	16,5%
Déploiement et configuration d'infrastructure dans le Cloud	15,5%
Gestion/simplification de localisation des données	6,8%
Mise en place d'une approche SASE	3,9%

Pour vos infrastructures : l'importance d'une stratégie globale

05

Éteindre des feux ou poser des rustines à certains endroits relève d'un autre temps. Au vu des formes multiples des cyberattaques, **il s'avère plus judicieux d'envisager une sécurisation globale**.

D'autant plus que les points d'entrée et les sources de danger se sont accrus avec la complexité et la multiplicité des systèmes informatiques et de leurs accès.

Qu'en est-il au niveau des infrastructures ?

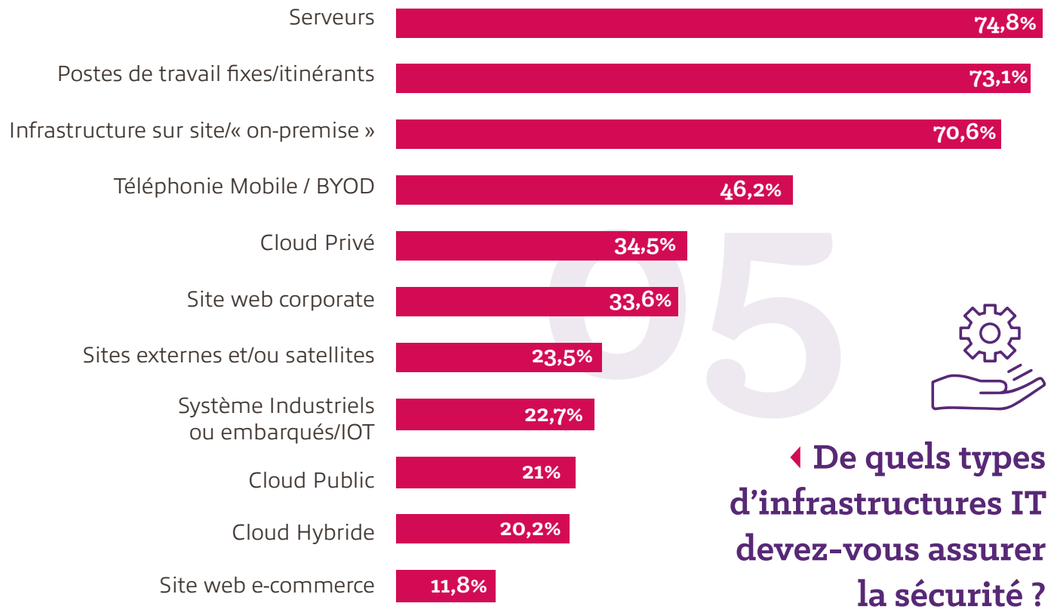
Pour nos répondants, en termes de sécurisation, la priorité porte sur 3 éléments : les serveurs, les postes de travail et l'infrastructure sur site.

(voir schéma 05)

En revanche, il est surprenant de constater que dans leurs réponses, **ni le site web ni l'éventuelle plateforme d'e-commerce ne sont repris en tant que principales priorités** pour les DSI en matière de sécurisation. Or, une stratégie efficace se doit de devenir de plus en plus globale, au vu de la multiplication des accès.

De fait, on accède aujourd'hui, à **un système informatique non seulement sur site mais également à distance**, et ce de plus en plus depuis la pandémie.

Cet accès à distance se réalise, dans le contexte de la généralisation du télétravail depuis soi, mais aussi à la suite de **l'accroissement du travail mobile** où les employés se connectent dans des espaces de coworking ou publics. Tous ces lieux n'offrent pas toujours la garantie d'un niveau suffisant de sécurité.



05

De quels types d'infrastructures IT devez-vous assurer la sécurité ?

Quant aux matériels utilisés et à leurs points d'accès, leur diversité et leur nombre compliquent également la prévention : certaines des administrations et entreprises de notre baromètre doivent en effet gérer 5.000 accès et plus. Et c'est bien là qu'une inquiétude peut naturellement apparaître, lorsque l'on constate :

1/3

des répondants n'a pas mis en place de stratégie globale de sécurité, ni partiellement, ni totalement.

06

Vos solutions : agir sur 3 axes

Un adage dit que le risque zéro n'existe pas. Certes. Mais 3 actions concomitantes peuvent être mises en place afin de parer à la majorité des attaques : la détection, la prévention et l'éducation. Développons.

LA DÉTECTION

Se doter de moyens de détection des attaques est une priorité majeure car, même en bâtissant des forteresses solides, des failles peuvent subsister, ne fut-ce qu'à la suite d'une erreur humaine.

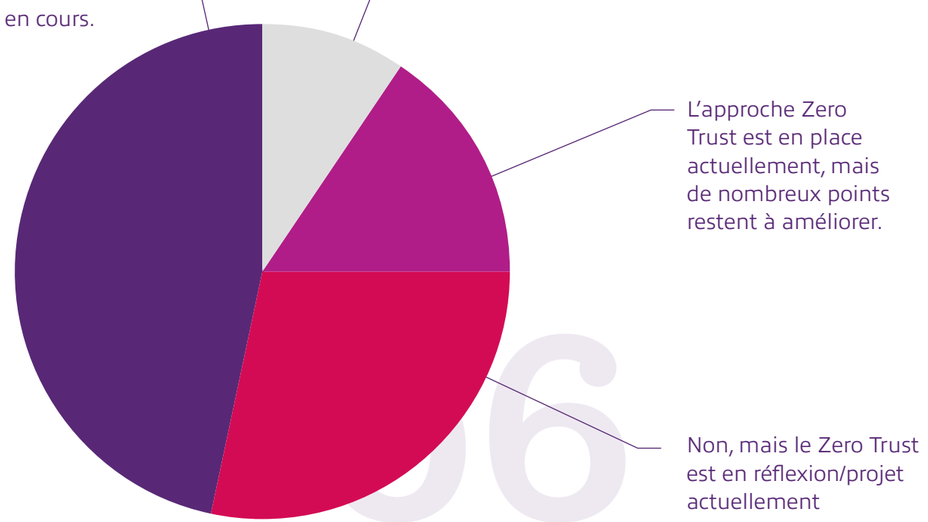
Pouvoir détecter à temps une contamination par un virus, une tentative de phishing ou une intrusion dans votre système informatique représente **un moyen de pouvoir rapidement empêcher une propagation**. Éviter les conséquences désastreuses d'une intrusion se fera au moyen d'outils de détection doublés de solutions à déployer afin de répondre rapidement à l'attaque constatée.

LA PRÉVENTION

En matière de cyberattaques, tout comme pour notre santé, il vaut mieux prévenir que guérir. Parmi les types d'approche et de solutions qui s'offrent aux responsables de la sécurité informatique, on peut citer :

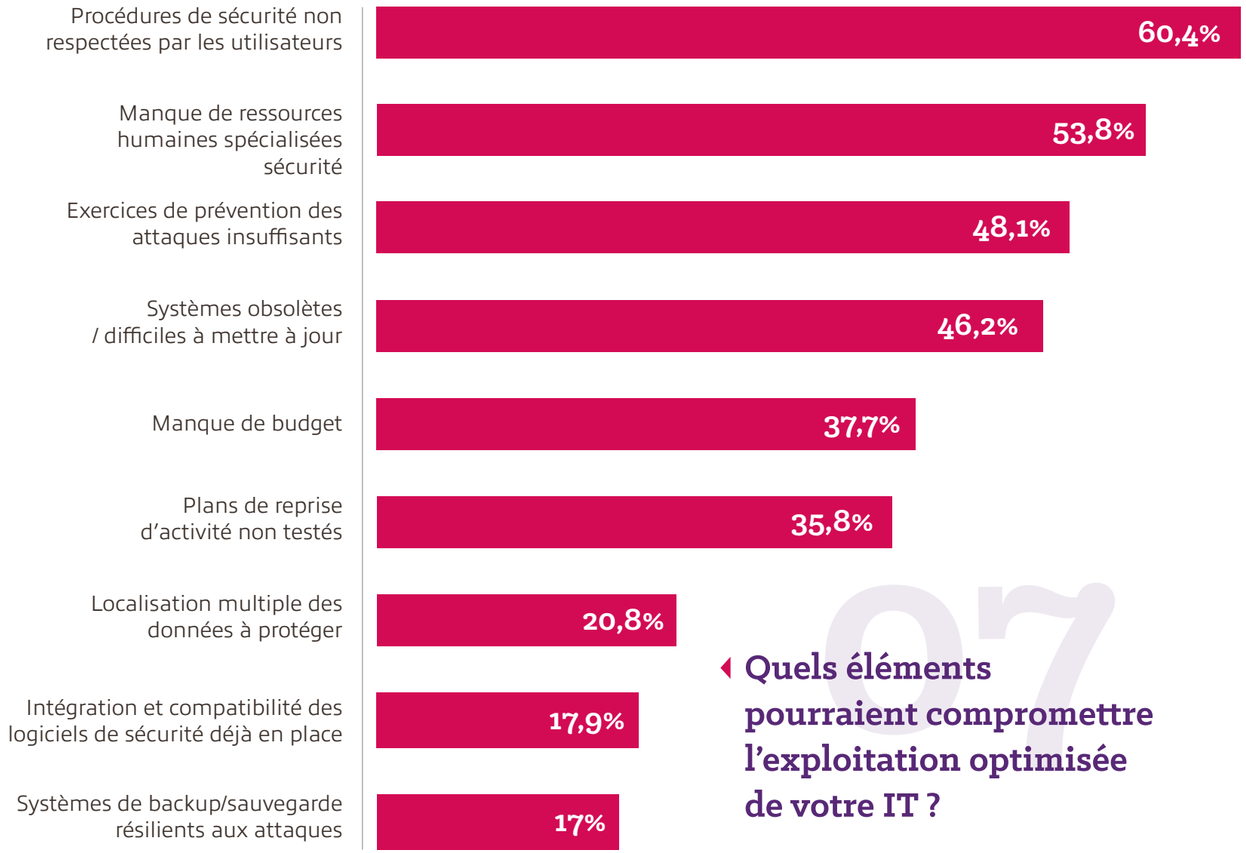
> La démarche "Zero Trust", un principe que plus de la moitié des DSI a déjà mis en place ou pense implémenter *(voir schéma 06)*. Il s'avère cependant que le Zero Trust ne soit pas toujours la panacée, eu égard à un côté parfois lourd et bloquant ressenti par certains utilisateurs.

> La mise en place de consoles de sécurité centralisées, un moyen de simplifier et piloter



la prévention. Or, 2/3 des répondants de notre sondage ne l'envisagent pas encore. Pourquoi ? Sans doute par **méconnaissance de l'efficacité d'une telle solution** ou par réticence en raison de sa complexité supposée. Quoi qu'il en soit, s'informer en vaut la peine.

Vos solutions : agir sur 3 axes



07

Quels éléments pourraient compromettre l'exploitation optimisée de votre IT ?

| L'ÉDUCATION

Tout système de protection aussi puissant soit-il ne peut prévenir à 100% la survenance d'une erreur humaine. D'ailleurs, les entreprises et administrations interrogées en sont conscientes puisqu'elles ont cité **3 facteurs humains en haut de leur liste des éléments à risque** *(voir schéma 07)*.

Ceci tend à démontrer l'importance de consacrer du temps et des ressources à ce troisième pilier de votre cybersécurité, à commencer par **la sensibilisation des collaborateurs**.

Communiquer, former, récompenser voire sanctionner sont autant de leviers à actionner pour assurer une cybersécurité répandue à tous les échelons.

Le message à passer s'avère être le même que celui dispensé dans le cadre de la prévention des accidents de travail : faire de la cybersécurité l'affaire de tous.

Conclusion

Il va de soi que **rien n'est acquis** contre les cyberattaques et que ces actions doivent évoluer constamment, au gré du développement de vos infrastructures, de vos RH, de votre (ré)organisation du travail et de vos supports d'accès.

De façon permanente, les DSI et RSSI se trouvent face à ce **challenge** : devoir agir plus vite que les cybercriminels. Dans ce contexte où le changement est permanent, il s'avère judicieux de **se faire aider**.

Les équipes spécialisées d'*Insight* et de *Symantec Broadcom* sont à votre disposition pour définir avec vous une approche complète pour votre organisation.

Contactez-nous pour obtenir un **audit** des éventuelles failles de votre système informatique ou pour réaliser des **exercices de crise** grandeur nature.

Nous pourrons alors vous conseiller pour **mettre en place de nouvelles solutions globales**, qui seules vous donneront les moyens de sécuriser davantage votre organisation dans son ensemble.

Symantec™ by Broadcom

Symantec Braodcom fournit **les meilleures solutions techniques** pour protèger les terminaux classiques et mobiles avec des **technologies innovantes** de réduction de la surface d'attaque, de prévention des attaques, de prévention des violations, de détection et de réponse. Toute cette protection est alimentée et **mise à jour en temps réel** par notre réseau mondial d'information, l'un des plus importants au monde.

Si l'accompagnement Symantec sur vos enjeux et projets SASE vous intéresse, visitez le site ou contactez nos experts cybersécurité.

Contact

Site web : insight.com
Tél. : 01 30 67 25 00

Insight Technology Solutions SAS | Le Crystalys 6 Avenue Morane Saulnier
78140, Vélizy-Villacoublay France | Enregistrée sous : RCS de Versailles B 397 888 330