

Guiddy

CYBERSÉCURITÉ

TEST D'INTRUSION

SENSIBILISATION

BLOG

PRENDRE UN RDV



CYBERSÉCURITÉ
PROTÉGEZ-VOUS SIMPLEMENT DU
RISQUE CYBER

CONTACTEZ-NOUS

Guiddy

CYBERSÉCURITÉ :

EN 2023, LES TPE ET LES PME SONT DANS LE VISEUR DES HACKEURS —
L'ANALYSE DE NICOLAS THORE, FONDATEUR DE GUIDDY

COMMUNIQUÉ DE PRESSE

La pandémie de Covid-19 a contraint les TPE/PME à effectuer leur transition numérique à marche forcée.

En peu de temps, sans y être préparées, elles ont dû s'adapter à l'essor du télétravail, à l'abolition des frontières pro/perso, et au changement d'attentes des jeunes diplômés, désormais beaucoup plus tournés vers la flexibilité et le bien-être.

Or, ce développement de la digitalisation est du pain béni pour les hackers : le nombre de cyberattaques (phishing, ransomwares...) n'a jamais été aussi élevé. Près de 9 entreprises sur 10 ont été victimes de cybercriminels en 2022 (*source*) et, en Europe, les cyberattaques ont augmenté de 26 % (source : étude Check Point Research).

Pourtant, si les pirates en ligne ciblent tout le monde, les entreprises sont loin d'avoir pris conscience de ces enjeux.

“On l'a vu en 2022, personne n'est épargné ! L'année dernière, Thales, les hôpitaux publics et privés, Orange Cyberdéfense, Deezer, Charlie Hebdo... se sont fait attaquer. Car si un hacker veut rentrer dans un système, il le fera.”, explique **Nicolas Thore**, fondateur de Guiddy.

D'ailleurs, la médiatisation de ces cas emblématiques ne doit pas faire oublier l'essentiel : en France, 52 % des victimes de cybercriminalité sont des TPE-PME.

Dans ce contexte, **Guiddy, le GPS de la cybersécurité, partage les bonnes pratiques à adopter pour réduire au maximum le risque numérique et les solutions pour agir avec efficacité.**



En 2023, la question n'est plus “Est-ce que je vais être attaqué ?” mais “Quand vais-je être attaqué ?” et surtout “Est-ce que je suis prêt en cas d'attaque ?”

Nicolas Thore, fondateur de Guiddy



EN 2023, LE RISQUE NUMÉRIQUE MAJEUR N'EST PAS QUE TECHNIQUE !

Le temps où quelques hackers isolés envoyaient des e-mails grossiers et truffés de fautes d'orthographe est révolu. En quelques années, ils ont évolué et ils sont désormais organisés comme des structures professionnelles.

Mais **les entreprises ne sont pas préparées à cette nouvelle menace.**

Nicolas Thore le constate à travers ses différentes rencontres professionnelles (associations d'entrepreneurs, événements d'information, pépinières d'entreprises, forums régionaux, événements cybersécurité) :

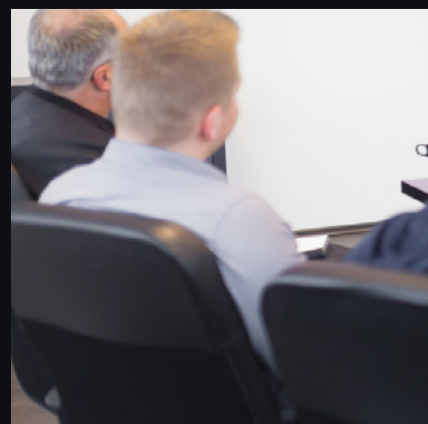
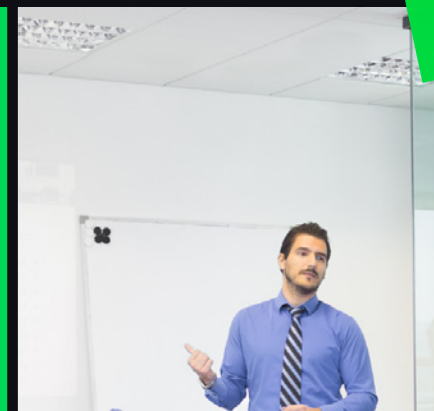


“Il y a une réelle méconnaissance des sujets liés à la cybersécurité et une ignorance des risques pour leur structure, alors que les conséquences peuvent être très graves pour leur activité.”

À titre d'exemple, il faut savoir que 64 % des décideurs IT croient encore que leur travail ne sera pas impacté par une attaque ransomware (étude Dell, décembre 2022).

C'est aussi pour cela que le risque numérique n'est pas seulement technique : il est aussi **humain et juridique.**

LUTTER CONTRE LES FUTURS CYBERATTAQUES



“

83 % des TPE/PME ne sont pas capables de se remettre des dommages financiers d'une cyberattaque (-27 % de CA en moyenne), surtout dans le contexte actuel ! Or, dans plus de 9 cas sur 10, les hackers réussissent à s'introduire grâce à un simple e-mail.

Nicolas Thore, fondateur de Guidy

LES BONNES PRATIQUES À ADOPTER POUR SE PROTÉGER DES HACKERS



SENSIBILISER LE PERSONNEL

Savez-vous que 92 % des cyberattaques (fuites de données, ransomwares, fraudes au président...) sont causées par une erreur humaine ?

Guiddy met ainsi en place des actions de sensibilisation pour **former les collaborateurs à repérer les arnaques**. Le plan de sécurité sera aussi testé pour avoir l'assurance de son efficacité.

EN SAVOIR PLUS



METTRE EN PLACE UNE POLITIQUE GLOBALE DE SÉCURITÉ

Il s'agit de construire une stratégie globale afin de **réduire le risque et l'impact d'une cyberattaque**.

Elle doit être structurée en 3 étapes :

- la prévention (état des lieux pour repérer les éventuelles portes d'entrée) ;
- la définition d'une politique de sécurité globale ;
- la sensibilisation des équipes.



PRÉVOIR DES PROCÉDURES EN CAS D'ATTAQUE

Plan de Continuité d'Activité (PCA) : Il vise à protéger l'ensemble des services de l'organisation. Il intervient, en principe, en amont pour prévenir les incidents et en diminuer l'impact et la gravité. Il peut s'agir, là encore, d'un événement gravissime pouvant paralyser le fonctionnement des services : la chaîne de production, la distribution, les ventes, etc.

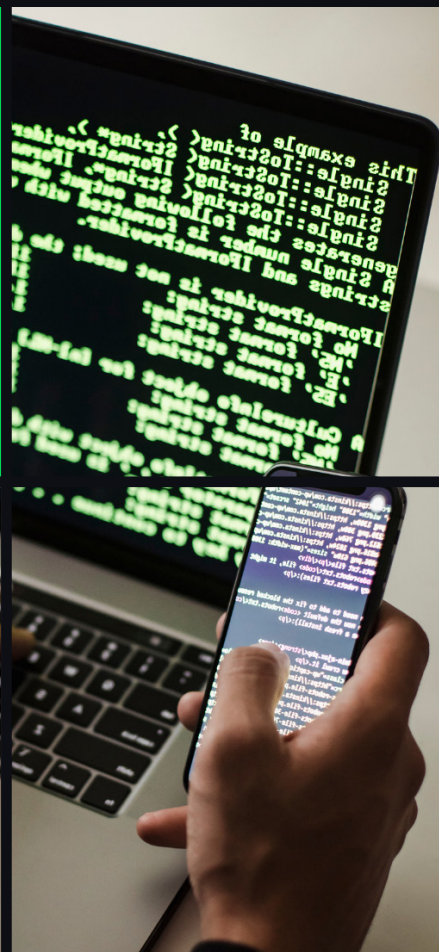
Plan de Reprise d'Activité (PRA) : initié par le service informatique, il regroupe toutes les mesures qui devront être appliquées, étape par étape, pour permettre aux utilisateurs du SI de retrouver l'accès aux données, aux applications, au réseau de l'entreprise et à internet.



Guiddy



**PENTESTER
PERMET DE
RENFORCER
LA SÉCURITÉ**



S'ENTRAINER PUIS TESTER LA ROBUSTESSE DU SYSTÈME ET DES PROCÉDURES

Parce que les applications web sont particulièrement fragiles, Guiddy propose **différents tests d'intrusion (Pentest) afin d'évaluer leur vulnérabilité.**

Ils permettent d'analyser le niveau de résistance du système d'information face à : suivre pour renforcer leur protection.

- ✓ Des attaques réalisées par un pirate depuis internet ou en interne.
- ✓ Des attaques réalisées lors de la fuite d'un compte utilisateur (compromission de poste de travail ou d'un sous-traitant).
- ✓ Des actes de malveillance interne ou des attaques réalisées sur une longue durée.

Son équipe d'auditeurs fournit ensuite un rapport présentant les points positifs et les informations nécessaires pour corriger les failles de sécurité. Un échange autour de ce rapport permet aux entreprises d'avoir des pistes concrètes à suivre pour renforcer leur protection.



TESTER LE SYSTÈME



GUIDDY, LE GPS DE LA CYBERSÉCURITÉ

Parce que la cybersécurité est un sujet anxigène pour les entrepreneurs, Guidy les accompagne de façon accessible pour les aider à gagner en maturité. Un peu comme un GPS mène les automobilistes vers un point précis et évite les embouteillages.

Guidés aussi bien techniquement que financièrement, ils sont déchargés de tout stress inutile.

AVEC EN PRIME, DE (GRANDS) PETITS PLUS :

- > **Une réponse adéquate et personnalisée** en fonction des besoins de chaque structure.
- > **Une approche humaine**, avec un réel suivi et une implication personnelle. L'idée est que tout le monde y gagne, en ayant notamment la satisfaction d'être protégé et en ayant les connaissances suffisantes pour ne plus être vulnérable.
- > **L'accessibilité et la transmission.** Guidy apporte et transmet des informations simples, compréhensibles. Au-delà des moyens technologiques, c'est aussi du savoir et de l'apprentissage sur la cybersécurité qui sont partagés.
- > **Un esprit de famille.** Au sein de Guidy, Nicolas Thore reproduit les expériences positives qu'il a vécues auparavant et il s'attache à incarner les valeurs qu'il souhaite véhiculer.
- > **Une large palette de services.** Guidy intervient de la sensibilisation à l'intégration, en passant par la création de sites web. La jeune pousse propose notamment un service de **DSI partagé** qui prend en charge la responsabilité de la transformation digitale de toute l'entreprise, à un coût maîtrisé.





À PROPOS DE NICOLAS THORE

Nicolas Thore est titulaire d'un diplôme de Chef de projet informatique.

Il a ensuite lancé sa première société, Sympel-net, dans la création de sites internet. Une expérience enrichissante, qui a duré 2 ans et demi, avant qu'il n'intègre en 2010 une entreprise dans le milieu médical. Recruté en tant qu'informaticien, il a ensuite gravi les différents échelons jusqu'à devenir Responsable des Systèmes d'Information. À ce poste, il a notamment développé un ERP/CRM complet.

Ayant le goût de la diversité et des challenges, Nicolas a poursuivi son évolution personnelle et professionnelle en rejoignant le monde de la sûreté internationale. Pendant deux ans, en tant que Responsable des SI, il a notamment eu l'opportunité de découvrir les spécificités de ce nouveau milieu, de gérer des interconnexions à l'international et de travailler sur des projets défense.

Il a ensuite poursuivi sa carrière en tant que Directeur des Systèmes d'information dans la cigarette électronique pendant deux ans et demi.

Fort de ces différentes expériences, Nicolas a renoué avec l'entrepreneuriat en octobre 2022 en fondant Guidy. Aujourd'hui, il ambitionne de continuer à développer Guidy pour recruter du personnel et intervenir dans toute la France.

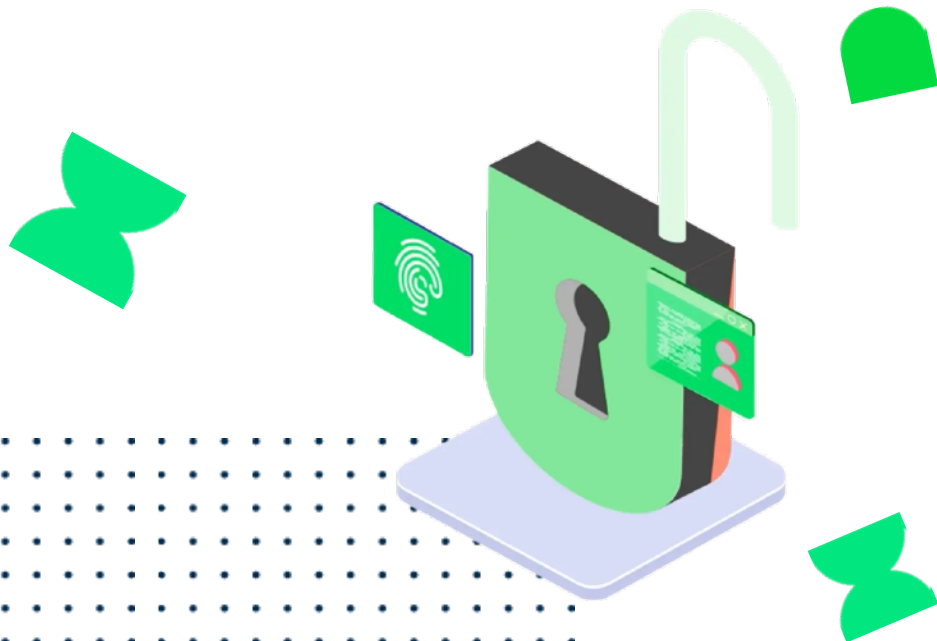
UN CONCEPT NÉ D'UN CONSTAT : IL Y A URGENCE À SENSIBILISER SUR LA CYBERCRIMINALITÉ

Fin 2021, la mère de Nicolas a été victime d'une tentative de Phishing par téléphone (vishing).

Elle l'a appelé un soir, paniquée.



Une personne se présentant comme représentant de sa banque, était au téléphone et insistait fortement pour qu'elle se connecte sur un site et fournisse différentes informations personnelles (pièce d'identité + carte bleue). Il lui faisait croire que son compte bancaire était en train d'être piraté...





Son interlocuteur appliquait des tactiques chères aux hackers :


- La méconnaissance des réglementations RGPD, puisque les informations sensibles n'ont pas à être communiquées par téléphone ;
- Et la pression instaurée par l'urgence.

En prenant conscience de la nécessité d'aider et de sensibiliser, Nicolas a eu l'idée de monter sa société dans la cybersécurité : le concept Giddy venait de naître !


POUR EN SAVOIR PLUS


 [Site web](#)

 [Guiddy](#)

 [Nicolas Thore](#)

CONTACT PRESSE

 Nicolas Thore

 contact@guiddy.fr

 01 89 27 24 06