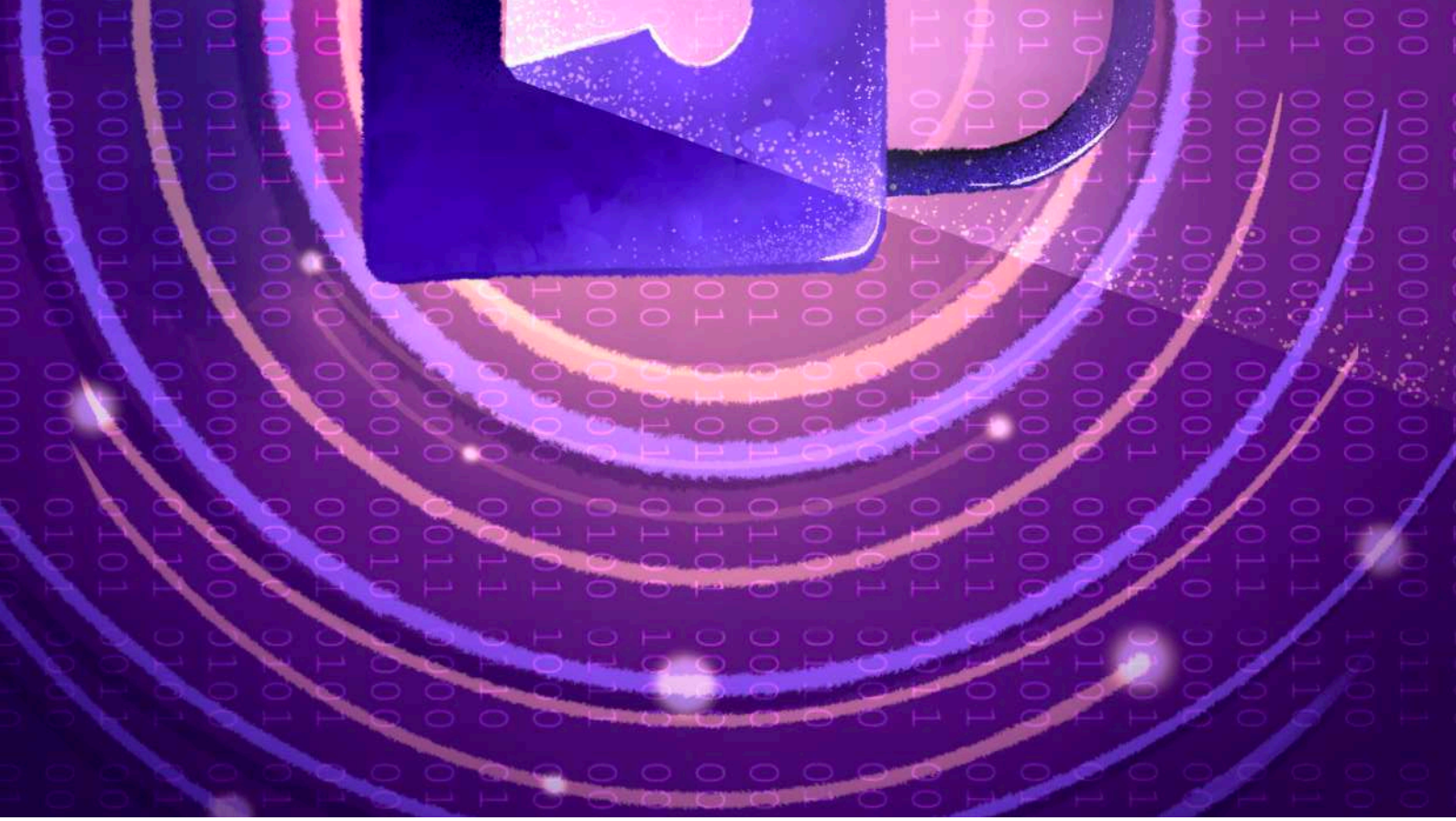


CYBER SÉCURITÉ

LIVRE BLANC

CODING THE FUTURE

Accréditations

Auteur

Marco Mehanna
SECURITY ADVISOR

Roberto Bindi
SECURITY ADVISOR

Gaia Conti
LEAD EDITOR

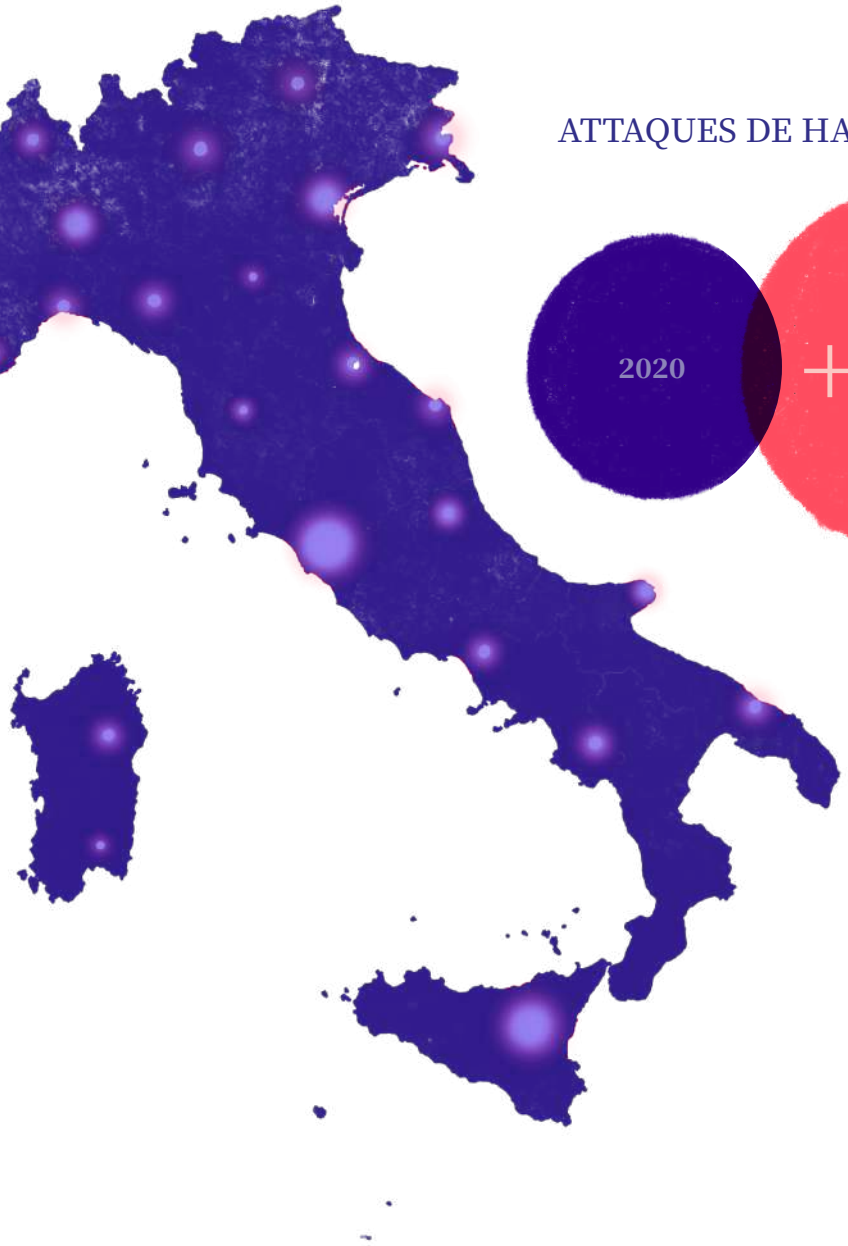
Ariele Pirona
VISUAL GRAPHICS

Sommaire

NUMÉROS

Comme le disait un vieux dicton, le seul moyen de maintenir un ordinateur complètement sécurisé est de l'éteindre. Et même cela pourrait ne pas suffire de nos jours, étant donné que la plupart des appareils sont connectés à Internet.
La réalité est qu'une sécurité parfaite (impliquant une certitude absolue de zéro perturbation) serait infiniment coûteuse et peu pratique.

L'objectif de la gestion des risques est d'optimiser l'allocation des ressources en minimisant à la fois le coût de la sécurité et les pertes dues aux risques.
La crise liée à la pandémie de COVID-19 a montré à quel point Internet et les ordinateurs en général sont importants pour les organisations et les entreprises de toutes tailles pour maintenir leur activité. Pour survivre à la pandémie et continuer leur activité, de nombreuses entreprises ont dû mettre en place des mesures de continuité commerciale telles que l'adoption de services cloud, la mise à jour des services Internet, l'amélioration des sites Web et la possibilité pour le personnel de travailler à distance. Pour ces raisons, la pandémie a posé de nouveaux défis en matière de sécurité informatique.



ATTAQUES DE HACKERS

En 2021, les organisations ont subi 50 % d'attaques de plus par semaine par rapport à 2020 - 2021
.

EN ITALIE

5000
Attaques par mois

167
Journalier

7
Horaire

Chaque fois que l'on entend le mot "piratage", la première chose à laquelle on pense, c'est qu'il s'agit de pratiques informatiques malveillantes.
Mais ce n'est pas le cas. Il n'y a pas de bons ou de mauvais hackers. Il existe des professionnels de la sécurité et des criminels informatiques.

NOTRE ÉTUDES DE CAS

RECHERCHE EN SÉCURITÉ

Adopter une approche éthique nous a permis de découvrir de nombreuses vulnérabilités dans de nombreux systèmes, comme celle identifiée fin 2017 : un défaut dans un composant du système de communication anonyme international, The Onion Router, connu sous le nom de Tor Browser. Plus précisément, Interlogica a identifié un bug dans le logiciel qui permettait à des tiers de découvrir l'identité des utilisateurs. Ce bug a ensuite été identifié comme TorMoil, signalé à l'entreprise et corrigé.

Un message "altéré" a provoqué la fermeture de Gmail, la messagerie Web la plus populaire au monde.

Pour les utilisateurs Mac avec Microsoft RDC installé, nous avons identifié un bug dans l'exécution du code à distance.

Ce bug que nous avons découvert affectait les appareils Mac OS X. Un JavaScript local permettait de contourner la quarantaine.

Nous avons découvert une anomalie dans SquirrelMail, qui permettait l'exécution de code à distance.

ADOPTER UNE APPROCHE ADÉQUATE

6 CONSEILS POUR PROTÉGER VOTRE ENTREPRISE AU MIEUX

1

RESTEZ INFORMÉ DES LOIS

Les lois sur la vie privée et la confidentialité évoluent constamment. Par exemple, le stockage et la gestion des données doivent être conformes à des réglementations telles que le RGPD. La mise à jour constante renforce la sensibilisation à la sécurité informatique et évite également des sanctions coûteuses en cas de non-conformité en cas de violation.

2

SÉGRÉGATION DES ENVIRONNEMENTS

Divisez le réseau interne en plusieurs sous-réseaux, chacun ayant des politiques de sécurité et des protocoles spécifiques. C'est la première étape pour prévenir la propagation latérale. Il s'agit d'une des pratiques les plus courantes pour limiter la surface d'attaque et contrer les cyberattaques.

3

APPLIQUEZ UNE POLITIQUE DE MOT DE PASSE

L'authentification, lorsque c'est possible, doit être centralisée. Cela signifie gérer les accès à travers des outils de gestion des identités auxquels une politique de mot de passe robuste doit être appliquée.

4

APPLIQUEZ DES STANDARDS DE DÉVELOPPEMENT SÉCURISÉ

Assurez-vous que les logiciels produits par votre entreprise et les logiciels utilisés suivent les directives de développement sécurisé (par exemple, les pratiques de codage sécurisé OWASP) et les bonnes pratiques du cycle de développement logiciel (SDLC)..

5

METTEZ À JOUR LES LOGICIELS ET LE MICROLOGICIEL

Gardez les systèmes et les applications à jour avec la dernière version fournie par le fournisseur. Cette pratique doit être effectuée régulièrement en utilisant un processus de gestion des correctifs interne et/ou des systèmes de mise à jour automatique.

6

SURVEILLANCE

Élaborez une stratégie de surveillance des systèmes informatiques et des réseaux, et développez des politiques de gestion des alertes. Analysez les journaux dans le but de détecter des activités inhabituelles qui pourraient indiquer une attaque.

CE QUE NOUS POUVONS FAIRE PUOR VOUS

NOS SERVICES

SÉCURITÉ PRÉDICTIVE

INTELLIGENCE DES MENACES CYBERNÉTIQUES

Notre équipe identifie les menaces provenant d'activités illicites d'exfiltration, à la fois directes et indirectes. Nous fournissons un soutien essentiel pour maintenir une surveillance constante de la sécurité de l'organisation et prévenir les menaces potentielles à long terme.

CONSCIENCE DE LA SÉCURITÉ

Notre mission est de sensibiliser et d'informer les individus sur l'importance de reconnaître différents types de menaces et de leurs conséquences potentielles, avant qu'elles ne puissent causer des dommages.

CONFORMITÉ

SUPPORT TECHNIQUE

Nous fournissons une assistance pour évaluer et mettre en œ uvre les mesures nécessaires pour être conforme aux normes GDPR. De plus, nous travaillons à améliorer la sécurité des systèmes, tant du point de vue logiciel que matériel, pour réduire au minimum les risques.

SÉCURITÉ PROACTIVE

TEST DE PÉNÉTRATION

Nous effectuons des analyses manuelles approfondies pour identifier et classer les vulnérabilités potentiellement exploitables par des agents malveillants. Nous testons votre système avec des attaques simulées et approfondies pour évaluer sa résistance.

EXAMEN DU CODE SOURCE

Nos experts analysent le code source de vos applications pour détecter les vulnérabilités potentielles, tant au niveau de l'infrastructure que de la logique. Nous utilisons des outils d'examen du code source et l'expérience de nos spécialistes pour garantir une sécurité maximale.

ÉVALUATION DES VULNÉRABILITÉS

Nous identifions et classons les vulnérabilités connues au sein des composants de l'entreprise, évaluant leur gravité pour vous aider à atténuer les risques.

ÉQUIPEMENT ROUGE

Notre équipe dédiée effectue des tests de type "équipe rouge" pour identifier les vulnérabilités informatiques et autres. Nous utilisons une variété de techniques, y compris des attaques de logiciels, de l'ingénierie sociale et d'autres méthodes pour évaluer votre sécurité en profondeur.

KNOWBE4

SOLUTIONS DE PARTENARIAT

Grâce à notre partenariat avec KnowBe4, nous offrons des services faciles à utiliser, gratuits et efficaces!

KnowBe4 est la principale plateforme au monde pour la sensibilisation à la sécurité et la simulation d'attaques de phishing.

Notre équipe de professionnels de la technologie relève les défis de la cybersécurité d'une manière unique, en mettant l'accent sur la construction d'un "pare-feu humain" solide.

Nous sommes fiers d'avoir été inclus dans le Magic Quadrant de Gartner en 2019 et d'avoir été confirmés en 2021 comme le choix des clients Peer Insights™ pour la qualité de la formation en sécurité informatique.

OUTILS GRATUITS POUR LA SÉCURITÉ DES TI

Mettez-les à l'épreuve avec des outils gratuits de sécurité informatique qui aident à identifier les problèmes d'ingénierie sociale, de spear phishing et d'attaques de ransomware parmi votre personnel d'entreprise.

Test de sécurité contre le Phishing
91 % des violations de données commencent par une attaque de spear phishing. Avec notre test, vous pouvez découvrir combien de vos employés pourraient être vulnérables au phishing et améliorer leur préparation.

Test des mots de passe violés
25 % des employés utilisent le même mot de passe pour tous leurs accès. Vérifiez si vos utilisateurs utilisent des mots de passe déjà compromis et prenez des mesures correctives rapidement.

Simulateur de Ransomware
Voulez-vous savoir si la protection des points de terminaison bloque effectivement les infections par ransomware et le cryptominage? Notre "RanSim" vous aide à évaluer rapidement l'efficacité de vos mesures de protection.

Contrôle de l'exposition des e-mails Pro
Soupçonnez-vous que les informations d'identification de vos employés ont été compromises ? Cet outil identifie les utilisateurs à risque au sein de votre organisation en analysant des milliers de bases de données de violations.

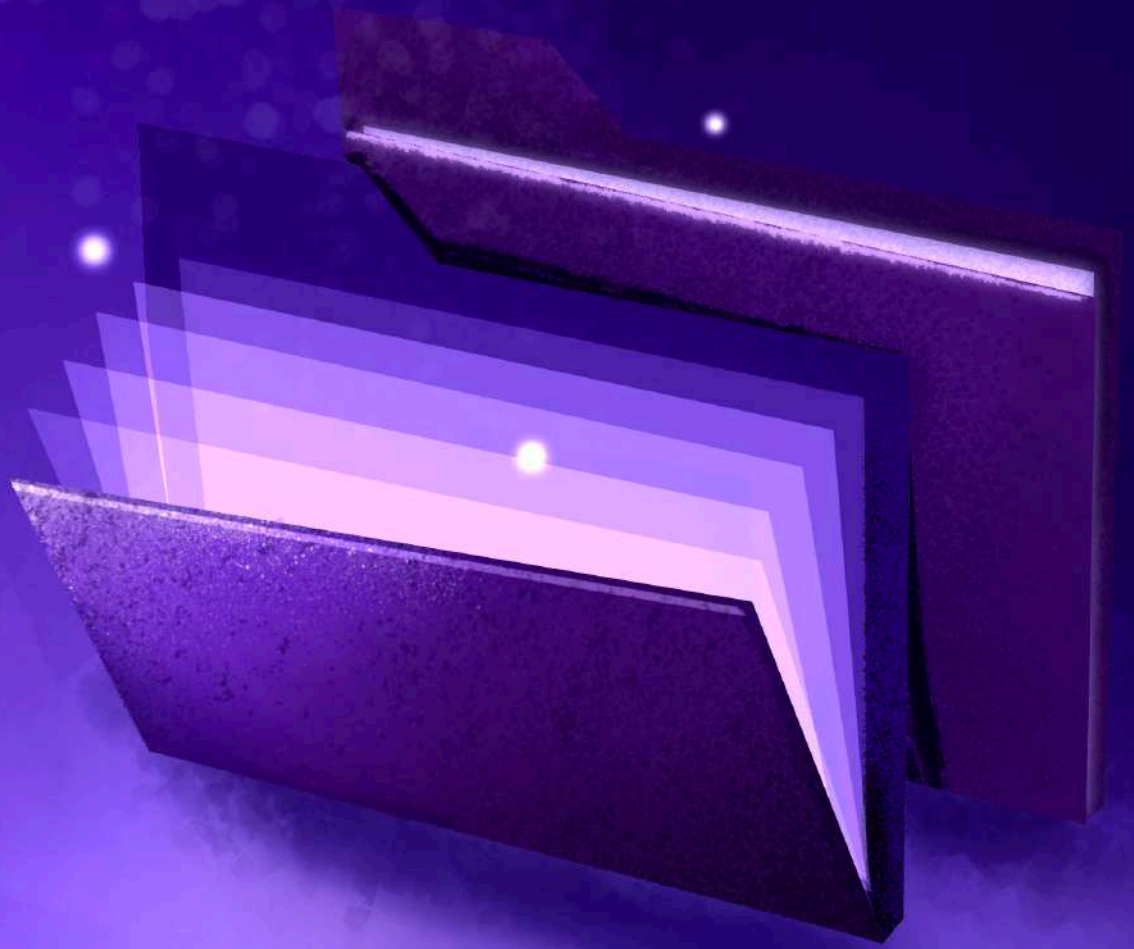
Évaluation de la sécurité de la messagerie
Les e-mails restent le principal vecteur d'attaque utilisé par les malfaiteurs. Notre évaluation de la sécurité de la messagerie (MSA) vérifie l'efficacité de votre serveur de messagerie pour filtrer et gérer les courriers indésirables.

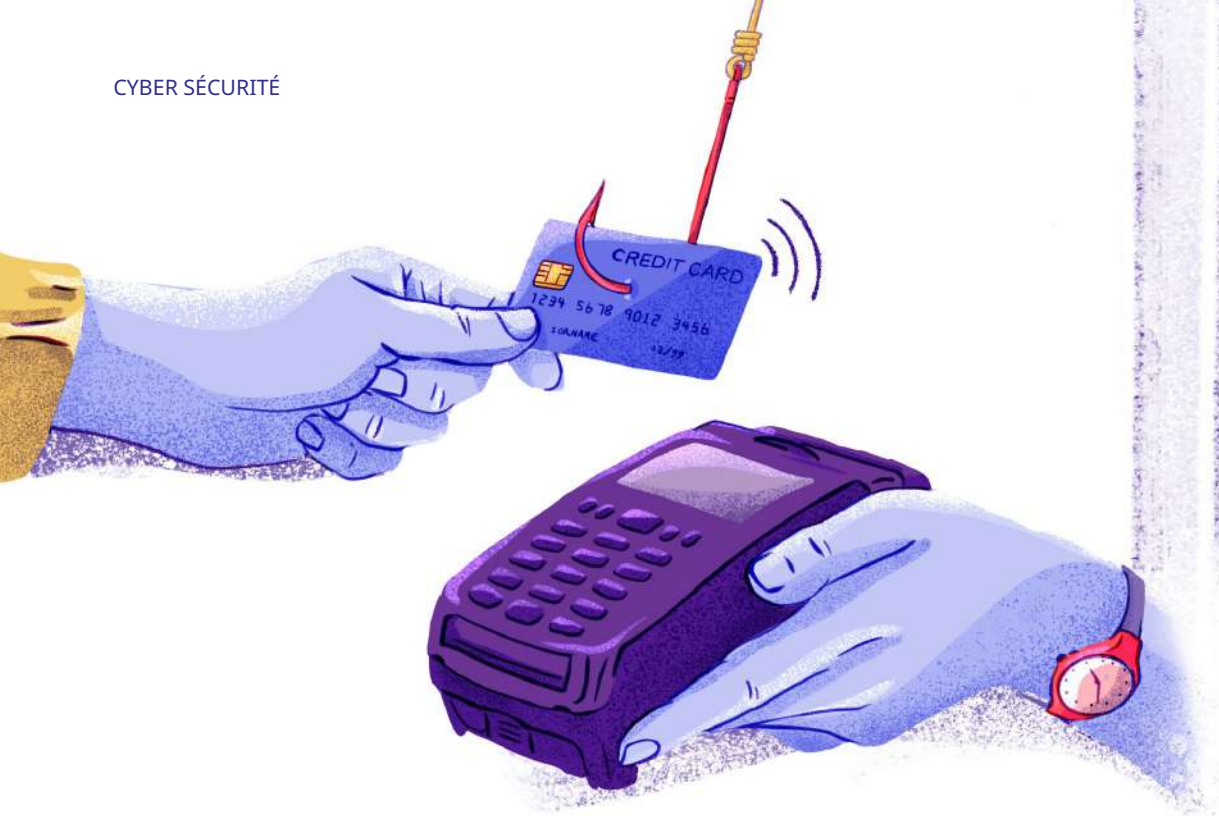
Portail de prévisualisation de Modstore
Accédez à la plus grande bibliothèque au monde de contenus éducatifs sur la sensibilisation à la sécurité informatique, comprenant plus d'un millier de modules interactifs, de vidéos, de jeux, d'affiches et de bulletins d'information.

Programme de sensibilisation à la sécurité automatisé
Créez un programme de sensibilisation à la sécurité personnalisé pour votre organisation, comprenant des activités, des conseils utiles et du contenu éducatif.

Doubleur de domaine
Identifiez et surveillez les domaines potentiellement malveillants qui pourraient être utilisés pour usurper votre domaine et mener des attaques.

ÉTDUDES DE CAS





ÉTUDE DE CAS

ARNAQUE DU CEO

L'arnaque du CEO est une fraude complexe dans laquelle un dirigeant ou un employé autorisé à effectuer des paiements est trompé pour payer une fausse facture ou effectuer un transfert non autorisé depuis le compte de l'entreprise.

QUELS SONT LES SIGNES ?

- E-mails ou Appels Non Sollicitésl
- Contact par des Cadres Non Habituels
- Demande de Confidentialité
- Sentiment d'urgence et de pression
- Demandes Inhabituelles ou Contraire aux Procédures
- Menaces ou Promesses de Récompense Inhabituelles

QUE FAIRE?

EN TANT QU'ENTREPRISE

- Soyez conscient des risques et veillez à ce que vos employés soient bien informés.
- Invitez votre personnel à traiter les demandes de paiement avec la plus grande prudence.
- Mettez en place des protocoles internes de paiement d'entreprise.
- Établissez une procédure de vérification pour confirmer la légitimité des demandes de paiement reçues par e-mail.
- Mettez en place un processus de signalement pour gérer les fraudes.
- Examinez les informations publiées sur le site Web de l'entreprise et limitez les informations sensibles. Soyez prudent dans l'utilisation des médias sociaux de l'entreprise.
- Renforcez et maintenez à jour les mesures de sécurité technologique .

EN TANT QU'EMPLOYÉ

- Suivez scrupuleusement les procédures de l'entreprise pour les paiements et les fournitures. Ne sautez aucune étape et ne cédez pas à la pression..
- Vérifiez toujours attentivement les adresses e-mail, en particulier lorsqu'il s'agit de données personnelles ou de facturation.
- En cas de doute sur un ordre de virement, consultez un collègue compétent ou un supérieur.
- N'ouvrez jamais de liens ou de pièces jointes suspects reçus par e-mail et évitez d'utiliser votre e-mail personnel sur les ordinateurs de l'entreprise.
- Limitez les informations et soyez prudent sur les médias sociaux.
- Évitez de partager des informations sensibles sur la structure interne, la sécurité ou les procédures de l'entreprise.

ÉTUDE DE CAS

VIOLATION DE DONNÉES

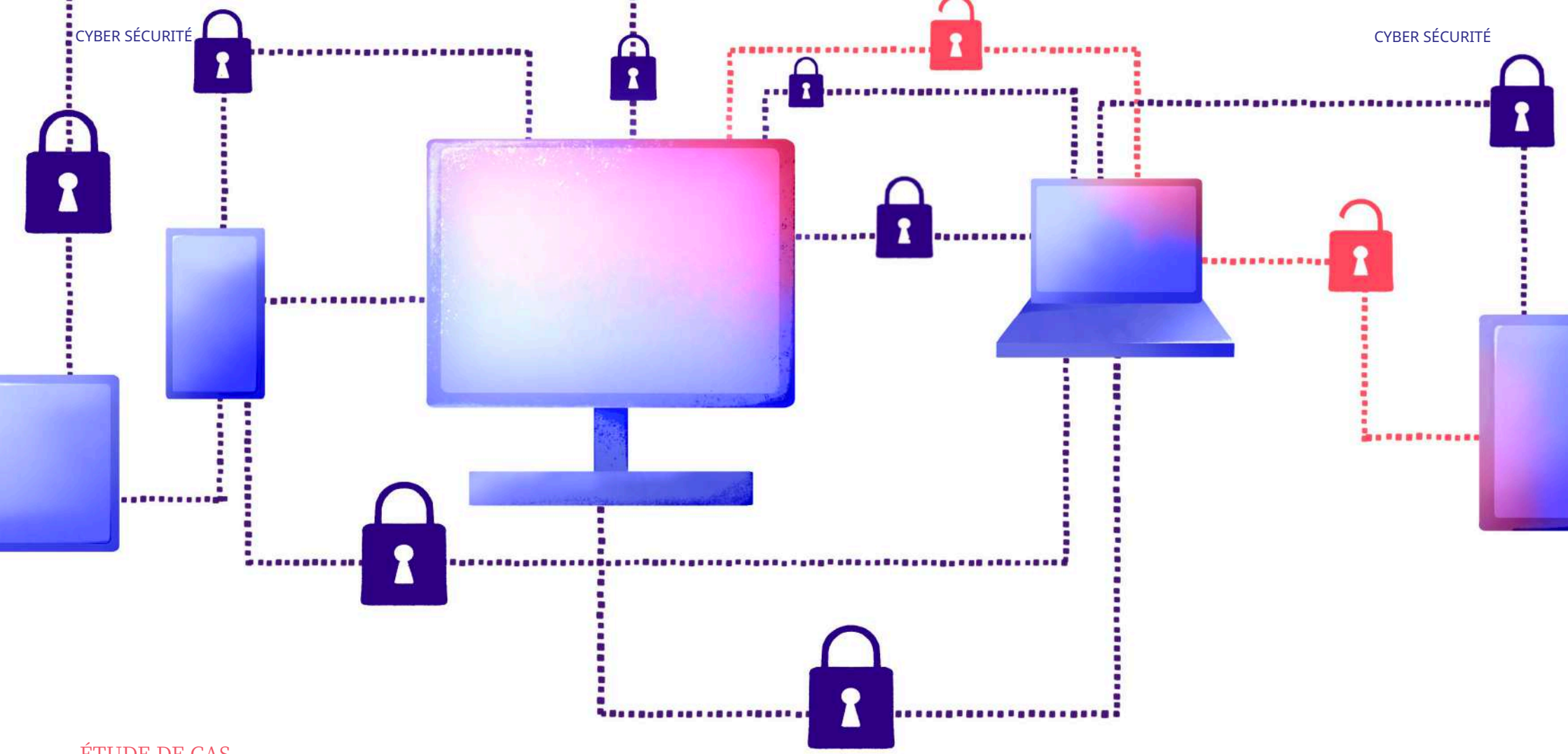
L'entreprise subit une importante exfiltration de données, qui sont ensuite rendues publiques sur Internet. À la suite d'enquêtes, il apparaît que les attaquants sont restés à l'intérieur de l'infrastructure informatique pendant des mois, en raison d'une sécurité périmétrique insuffisante et de l'absence de systèmes de surveillance. La violation de données n'est découverte qu'au moment de la publication des données.

QUE FAIRE?

EN TANT QU'ENTREPRISE

- Fournissez à l'entreprise des systèmes de protection périmétrique et de surveillance.
- Mettez en place des politiques de segmentation du réseau pour éviter que l'attaquant ne puisse se déplacer librement sur le réseau interne.
- Effectuez des activités de "Red Teaming" en faisant appel à un groupe d'experts qui simuleront des scénarios d'attaque réels à l'intérieur du périmètre de l'entreprise afin d'identifier d'éventuelles faiblesses et de procéder à une évaluation précise des risques.

CYBER SÉCURITÉ



ÉTUDE DE CAS

VULNÉRABILITÉS CONNUES

L'infrastructure de l'entreprise a été partiellement compromise, tant en termes d'intégrité que de disponibilité des services offerts. Les applications de l'entreprise utilisent principalement le framework Struts, et la version installée est affectée par une vulnérabilité connue, de gravité élevée et facilement exploitable.

QUE FAIRE?

EN TANT QU'ENTREPRISE

- Mettez en place un pare-feu d'applications Web pour protéger l'infrastructure.
- Effectuez une évaluation des vulnérabilités pour identifier les vulnérabilités connues présentes dans les composants utilisés.
- Mettez en place un processus de gestion des correctifs pour effectuer des mises à jour structurées sur tous les composants utilisés.
- Effectuez régulièrement des tests de pénétration sur les applications et les serveurs. Effectuez une analyse du code source avant chaque déploiement en production.

GLOSSAIRE

ANTIVIRUS

Un antivirus est une application logicielle qui aide à protéger l'ordinateur contre les virus. C'est une recommandation standard pour tout ordinateur, qu'il s'agisse d'un ordinateur d'entreprise ou personnel. Ils sont généralement équipés:

- Multi Appareils, ce qui signifie que vous pouvez l'utiliser pour protéger votre ordinateur, votre téléphone portable et votre table.
- Protection multi-menaces, ce qui signifie qu'il vous protège contre différents types de cyber-menaces.
- Contrôle parental, qui vous permet de contrôler ce que vos enfants peuvent faire sur votre ordinateur.
- Pare-feu, ajoutant une couche de défense entre votre ordinateur et l'internet.
- Un outil de suppression de virus pour vous aider si votre ordinateur est infecté.

CRYPTOGRAPHIE

La cryptographie est une forme de protection des données. Le processus de cryptographie consiste à utiliser des codes et des clés complexes pour crypter ou verrouiller les données, les rendant presque inutiles à moins de disposer de la clé pour les décrypter ou les déverrouiller. La cryptographie est utilisée pour protéger les informations sensibles et sécuriser l'ordinateur physique.

—

CYBER THREAT INTELLIGENCE

La Cyber Threat Intelligence est un outil pour adopter des outils de défense spécifiques contre les attaques potentielles et pour identifier de nouvelles failles au sein du réseau de l'entreprise. Elle aide à prévenir les attaques des cybercriminels.

—

VIOLATION DE DONNÉES

Une violation de données se produit lorsque des données personnelles ou d'entreprise sont compromises et qu'un pirate informatique y a accès. Cela peut entraîner le vol de données ou l'introduction de logiciels espions dans les systèmes.

—

PARE-FEU

Un pare-feu agit comme une barrière entre l'ordinateur et Internet pour protéger l'ordinateur et les données. Il existe des pare-feu physiques et virtuels, et à la fois Windows et Mac disposent de fonctionnalités de pare-feu intégrées.

PARE-FEU HUMAIN

L'élément humain de la cybersécurité est essentiel. Il est important d'éduquer les personnes à identifier les escroqueries informatiques et à reconnaître les attaques potentielles.

—

TEST DE PÉNÉTRATION

Le test de pénétration, ou Pentest, est une évaluation du niveau de sécurité des actifs de l'entreprise, y compris les serveurs et les applications. Il aide à repérer les failles de sécurité et les problèmes de configuration.

—

PHISHING

Le phishing est un type d'escroquerie dans lequel un malfaiteur tente de tromper la victime pour qu'elle fournisse des informations personnelles par le biais de communications numériques frauduleuses.

—

RANSOMWARE

Le Ransomware est un virus qui crypte les fichiers de l'ordinateur ou du réseau de l'entreprise et demande une rançon pour les déverrouiller.

—

CONSCIENCE DE LA SÉCURITÉ

La conscience de la sécurité est la connaissance et l'attitude des personnes

envers la protection des ressources informatiques. Il est important d'éduquer les personnes à reconnaître les menaces informatiques.

—

INGÉNIERIE SOCIALE

L'ingénierie sociale repose sur la manipulation des personnes pour obtenir des informations ou un accès non autorisé aux systèmes informatiques.

—

VULNÉRABILITÉ

La vulnérabilité fait référence à toutes les zones où une entreprise pourrait être vulnérable à une attaque informatique. Cela peut inclure des correctifs de sécurité manquants, des politiques de sécurité inadéquates, des failles de sécurité matérielles ou logicielles, et bien plus encore.

.

WE ARE INTERLOGICA

Nous nous spécialisons dans le conseil en technologie en intégrant la stratégie et les logiciels. Nous vous accompagnons dans la conception, la mise en place et la gestion de divers environnements informatiques pour vous permettre de prospérer dans un marché en constante évolution. Ensemble, créons un parcours personnalisé.

Suivre sur

in company/Interlogica
@interlogici
f @Interlogica

Plus d'info

interlogica.it
info@interlogica.it

Accréditations

CSQ ISO 9001
CSQ ISO/IEC 27001

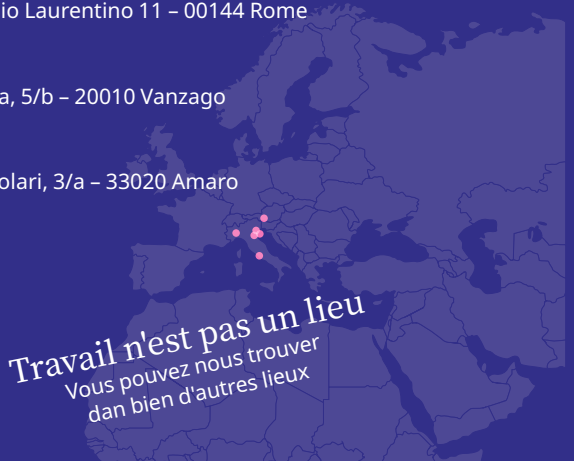
Contacts & bureaux

Venise
Via Miranese, 91/4 – 30174 – Mestre (VE)
+39 041 5354800

Rome
Via G. Coppola di Musitani 34 – 00139 Rome
Via del Poggio Laurentino 11 – 00144 Rome

Milan
Via Pregnana, 5/b – 20010 Vanzago

Udine
Via Fratelli Solari, 3/a – 33020 Amaro



Travail n'est pas un lieu
Vous pouvez nous trouver dan bien d'autres lieux

Prenez contact avec nos experts

Renforcez vos barrières. Dynamisez votre stratégie et investissez dans la défense, la sensibilisation et la connaissance pour développer une culture de la cybersécurité.

Interlogica

CODING THE FUTURE

interlogica.it