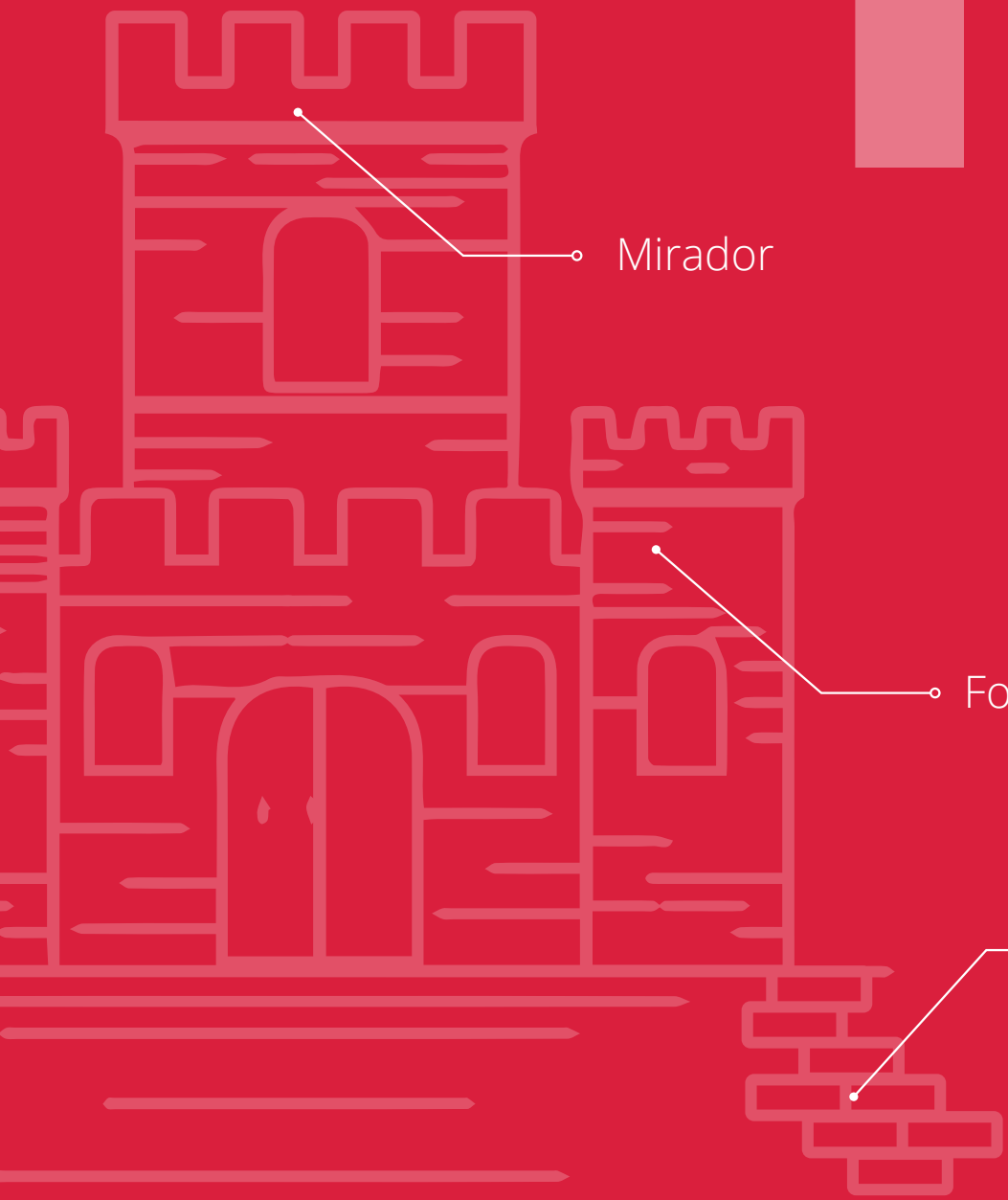
Evaluez la
# cybersécurité
de votre entreprise sur

# 15
points




Uniwan SRL
CHARLEROI • PONT-À-CELLES • BRUXELLES
+32 71 84 92 96 | uniprotect@uniwan.be | www.**uniwan**.be

UNIWAN
Next Technology Provider

## FONDATIONS

☐ 3 3 3

### #01 Etat des lieux

Identifiez les données et applications vitales pour votre entreprise : leur protection doit être prioritaire pour prévenir tout arrêt d'activité. Quels sont les éléments de votre système informatique ? Combien de PC, de NAS, de Serveurs, d'imprimantes et d'équipements réseau, tous devront être revus.

☐ 1 3 2

### #02 Sauvegardes

Garantissez la disponibilité de vos données en suivant la règle de backup 3-2-1-1-0 : conservez 3 copies sur 2 supports différents, 1 dans le cloud et 1 en local. Vérifiez le 0 erreur lors des tests de récupération. Rappelez-vous, le stockage cloud n'est pas systématiquement sauvegardé.

☐ 1 3 2

### #03 Protection du mail (Anti-Spam/Phishing)

Sécurisez votre mail, il doit être «authentifiable» via SPF, DKIM, DMARC. La plupart des attaques commencent par un mail. Protégez-vous contre le spam et le phishing. Les liens et pièces jointes doivent être désarmés par un système de protection.

☐ 2 3 1

### #04 Protection des PC/SRV (~~Antivirus~~ & EDR)

Protégez vos ordinateurs des malwares, virus et cyberattaques avec des solutions modernes (Endpoint Detection & Response). Aujourd'hui, les simples antivirus sont dépassés face aux scripts des cyberattaques. Un EDR isole du réseau une machine suspecte le temps de la réparer.

☐ 3 3 3

### #05 Formation des utilisateurs

Formez vos utilisateurs. En plus de leur enseigner les fondamentaux, vos politiques et procédures, utilisez des posters de rappel dans toute l'entreprise pour une sensibilisation continue et un renforcement de la 'Security Awareness'. Gardez vos utilisateurs «Aware».

☐ 3 1 2

### #06 Protection des mots de passe

Appliquez des politiques de mots de passe. Ne laissez aucun mdp d'usine (NAS, Switch,...). Verrouillez les écrans après un certain délai. Stockez vos mdp dans une base de donnée cryptée et sécurisée par MFA (#9) qui détecte les brèches sur le darkweb.

## FORTIFICATIONS

☐ 2 3 2

### #07 Mise à jour (updates)

Maintenez vos PC, Serveurs, NAS, imprimantes et équipements réseau à jour. Ne ratez pas les mises à jour critiques. Faites-vous aider par des agents automatisés pour protéger vos PC/Serveurs des dernières attaques en supprimant les dernières vulnérabilités connues.

☐ 3 2 1

### #08 Sécurité réseau (Segm, Filtrage, DNS)

Segmentez le réseau en zones spécifiques (invité, pro, prod, cam). Installez un pare-feu moderne pour filtrer le trafic entre ces segments. Utilisez un DNS sécurisé pour prévenir les manipulations malveillantes, réduisant ainsi significativement le risque de contamination globale de l'entreprise.

☐ 3 1 1

### #09 Authentication Multi-Facteurs (MFA)

Utilisez l'authentification multiple partout où vous le pouvez, sur vos sites bancaires et même sur les réseaux sociaux. Le MFA sollicite votre Smartphone et la biométrie. Elle ajoute une couche de protection supplémentaire même si votre mot de passe est volé.

☐ 3 3 2

### #10 Paramètrage de sécurité

Sécurisez les configurations (Security Configuration Baseline), en évitant les configurations par défaut trop vulnérables. Supprimez les applications superflues (striping) et ajustez rigoureusement les paramètres des éléments restants (hardening) pour prévenir les attaques et faiblesses. Cette règle s'applique à tout.

☐ 3 3 1

### #11 Sécurité des équipements mobiles

Optez pour un MDM (Mobile Device Management) efficace pour contrer les cybercriminels visant smartphones et tablettes. Sécurisez, chiffrez, localisez et, si nécessaire, effacez les données pour éviter que la négligence envers ces appareils ne devienne une vulnérabilité majeure.

☐ 3 3 1

### #12 Chiffrement

Adoptez une stratégie proactive en matière de cryptage, en assurant l'encryption des fichiers au repos et en déplacement, particulièrement sur les équipements mobiles. L'encryption 'native' est largement disponible sur les devices et dans le cloud, mais son activation reste cruciale.

## MIRADORS

☐ 3 3 3

### #13 Évaluation de la sécurité globale

Planifiez un «security assessment» rigoureux pour établir une base de références solides et éliminer les vulnérabilités existantes. Engagez des spécialistes pour un test de pénétration (pentest), afin d'identifier et de corriger les faiblesses restantes. Demandez-vous : quand a-t-on effectué la dernière évaluation de sécurité ?»

☐ 1 3 3

### #14 Centre de télésurveillance

Souscrivez aux services d'un Centre de Télésurveillance en Cybersécurité (SOC), qui centralise et analyse en continu les événements de sécurité. Grâce à l'I.A. et à des agents qualifiés, il détecte et neutralise proactivement les menaces, protégeant ainsi ordinateurs, serveurs, cloud et tous les points vitaux de votre réseau 24h/24.

☐ 3 3 3

### #15 Assurance Cyber Risques

Pour le risque résiduel, pensez à prendre une assurance pour protéger votre revenu et votre business.

## Quel est votre score en **cybersécurité ?**

...../15

| | |
|---|---|
| Confidentialité | ...../34 |
| Intégrité | ...../37 |
| Disponibilité | ...../29 |
| TOTAL | ...../100 |