PROTÉGER MON ENTREPRISE DES CYBERATTAQUES...

VOL DE DONNÉES, ESCROQUERIE AU FAUX RIB, BLOCAGE DE VOTRE SYSTÈME D'INFORMATION...QUE FAIRE SIMPLEMENT ET RAPIDEMENT ?

DÈS AUJOURD'HUI SÉCURISER VOTRE SYSTÈME D'INFORMATIONS ET VOS DONNÉES

- *Mettre en place ou renforcer les protections existantes (mots de passe, droits d'accès etc.)*
- *Sécuriser les données stratégiques (comptes clients, formules et brevets, données de gestion)*
- *Mettre en place les bons réflexes et les bonnes pratiques pour tous vos collaborateurs*

Vos données, votre patrimoine immatériel sont des biens précieux à protéger avec rigueur.

CCI AIX MARSEILLE PROVENCE

DEMAIN, EN FAIRE UN ATOUT POUR VOTRE ENTREPRISE !

Vous répondez à des marchés, vous êtes sous-traitant ?

Les donneurs d'ordres sont de plus en plus attentifs à la manière dont vous sécurisez vos données, notamment dans des secteurs sensibles (finance, nouvelles technologies) ou très concurrentiels ; prochainement de plus en plus d'appels d'offre comporteront une clause cybersécurité qui deviendra un incontournable.
Démontrer l'image d'une entreprise sécurisée est d'ores et déjà un avantage concurrentiel.

Vous souhaitez contracter une assurance Cybersécurité ?

Si votre entreprise adopte des mesures préventives, votre police d'assurance en sera minorée. Certaines assurances ne pourront pas être souscrites sans une politique cybersécurité solide.

PRENDRE EN COMPTE LE RISQUE CYBER EST VITAL

Votre CCI est là pour vous aider à mettre en place des mesures pratiques et simples pour sécuriser vos biens et choisir les stratégies les plus intéressantes pour vous.

Tout au long de l'année 2022 des actions sont prévues pour vous épauler.
Contact mail : patricia.bohbot@cciamp.com

Programme du 1er trimestre 2022

27 Janvier

Réunion d'information/ sensibilisation gratuite avec une experte en management de la sécurité des données numériques.

Présidente de l'Association de Criminologie du bassin Méditerranéen (ACBM) et membre actif de l'Association des réservistes du chiffrement et de la sécurité informatique (ARCSI).

- Enjeux de la cybersécurité
- Faire face à la menace croissante
- Anticiper les cyberattaques
- Conséquences d'une cyber attaque

22 et 23 Février

Formation sur 2 jours (financement possible par votre OPCO)

Programme :

- Connaissance et détection des cyber menaces
- Sécurisation du parc informatique et protection technique
- Impacts du RGPD sur la cybersécurité
- Usage collaborateurs et Hygiène comportementale
- Préparer la gestion de crise
- Analyse des contrats d'assurance cyber risques

Mars

Colloque SECNUMECO au Palais de la Bourse, en partenariat avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSII) et le Service de l'Information Stratégique et Sécurité Economique (SISSE).

Vous y rencontrerez l'ensemble des acteurs Cyber de la région. L'occasion de découvrir le capital digital de votre entreprise et vous informer sur les manières d'écarter les dangers numériques. (Programme à venir)

Pour en savoir plus sur le sujet de la Cybercriminalité et les risques : cciamp.com

*Extraits de témoignages recueillis (« flash » d'ingérence économique de la DGSI)

LES ATTAQUES LES PLUS COURANTES

Vol de données :

« Profitant de la généralisation du télétravail pour tous les salariés d'une entreprise, un cybercriminel a réussi à usurper l'identité d'un membre du service informatique et a lancé une campagne de phishing aux télétravailleurs pour récupérer leurs mots de passe et accéder au réseau. »*

Escroquerie au faux RIB :

La réception d'un RIB semblant provenir d'un de vos fournisseurs, ou partenaires extérieurs par suite d'un changement de compte bancaire. Mais qui en fait est un faux.

Blocage de votre système d'information :

Un virus bloque votre ordinateur contre une rançon.

Interception de données confidentielles sur des supports mobiles (smartphone, tablette...) :

Un dirigeant d'entreprise française en déplacement s'est connecté avec son ordinateur professionnel à plusieurs réseaux wifi (hôtel, aéroport, etc.) afin d'envoyer des courriels sensibles relatifs à un appel d'offre. Les échanges ont été interceptés et son concurrent a pu remporter le marché.

Action de sabotage :

Des droits d'accès toujours ouverts malgré un contrat arrivé à terme (ex : maintenance).

Risque d'image et dénigrement :

« Une PME, spécialisée dans le matériel sanitaire, a été la victime d'une attaque informatique après la parution d'un article de presse. Un cybercriminel a piraté l'adresse électronique officielle de l'entreprise pour contacter des sociétés. Profitant de la notoriété de sa victime, il a proposé à ses cibles du matériel sanitaire. »*

Piratage téléphonique :

Août 2019, veille d'un week-end, une entreprise marseillaise a été victime de « phreaking » - exploitation des infrastructures téléphoniques – 108 000 appels ont été émis pour 260 000€.

LA QUESTION N'EST PAS DE SAVOIR SI VOTRE ENTREPRISE PEUT ÊTRE ATTAQUÉE MAIS PLUTÔT QUAND ?

*Extraits de témoignages recueillis (« flash » d'ingérence économique de la DGSI)