

## **Netwrix : Les 7 prévisions cybersécurité pour 2021**

### **Internet**

Posté par : JPilo

Publié le : 2/12/2020 15:00:00

Netwrix, fournisseur de cybersécurité qui simplifie la sécurité des données, dévoile les prévisions et principales tendances qui auront un impact sur la sécurité des entreprises en 2021 et au-delà. Ces projections résultent de la transformation numérique et de la nouvelle normalité imposées par la pandémie et l'adoption du télétravail.

Netwrix recommande ainsi aux professionnels de l'informatique et de la sécurité de repenser leurs stratégies de gestion des risques et de poursuivre le suivi des opérations en tenant compte de ces sept prévisions.

### **1. Les ransomwares causeront des dommages plus importants afin de motiver les paiements.**

La prochaine génération de ransomwares sera conçue pour causer des dégâts plus difficiles à réparer, afin de forcer les organisations à payer la rançon. Le « brick » des appareils (désigne une mort logicielle ou matérielle d'un produit) par la modification du BIOS (c'est-à-dire l'ensemble de fonctions, contenu dans la mémoire morte de la carte mère d'un ordinateur) ou d'autres micrologiciels, en est un exemple.

Les cybercriminels se tourneront également vers de nouvelles cibles, telles que la technologie opérationnelle et les dispositifs IoT ; car les attaques auront alors un impact beaucoup plus visible sur le monde physique.

### **2. Les erreurs de configuration du Cloud seront l'une des principales causes des violations de données.**

Une transition rapide vers le Cloud et un manque de compréhension du modèle de la responsabilité partagée se retourneront contre les entreprises en 2021.

En effet, la rapidité à laquelle s'est déroulée l'adoption, couplée à la priorisation de la productivité par rapport à la sécurité, a rendu inévitable des erreurs de configuration, qui se traduisent par une surexposition des données.

### **3. Les cybercriminels cibleront de plus en plus les fournisseurs de services.**

Le manque d'experts dans le domaine de la cybersécurité amènera les entreprises à se tourner vers les fournisseurs de services managés (MSP).

Dans ce contexte, les pirates informatiques initieront des attaques ciblées contre ces MSP pour avoir accès, non plus qu'à une seule organisation, mais à la totalité des clients de ces derniers.

### **4. La transformation numérique massive en 2020 aura un impact sur la cybersécurité en 2021.**

En 2020, les organisations ont dû s'adapter rapidement à de nouvelles méthodes de travail et à la mise en place de nouveaux dispositifs ; sans toujours bénéficier de l'expérience et du temps nécessaire pour déployer et tester ces dispositifs.

Pour cette année à venir, les branches de sécurité causées par les évènements commises au cours de cette transition rapide seront donc exploités, et de nouveaux types de violations de données, comme les récents piratages de Twitter, seront à constater.

### **5. La preuve de la valeur dirigera les décisions des entreprises.**

Les dirigeants tenteront de trouver des mesures spécifiques permettant de déterminer la valeur ajoutée des services et des mesures de sécurité mis en place. L'objectif est d'évaluer la pertinence des investissements réalisés et de ceux à venir.

### **6. Les entreprises devront trouver un équilibre entre leur cybersécurité et leurs besoins opérationnels, tout en privilégiant le facteur risque.**

Les difficultés liées à la pandémie obligeront les organisations à évaluer leurs priorités. Les équipes IT devront notamment trouver le bon équilibre entre la sécurité élevée et les besoins de l'entreprise, comme la flexibilité et l'accessibilité.

Les attentes évolueront de l'idée irréaliste de garantir une sécurité à 100 % à l'ambition de déterminer et de respecter des niveaux acceptables de risque et de résilience.

### **7. Les assurances et la réglementation favoriseront l'adoption massive de meilleures pratiques de sécurité opérationnelle.**

Afin de réduire au minimum le risque d'encourir de lourdes amendes en cas de non-respect de la réglementation en vigueur, les entreprises se tourneront vers la cyber-assurance.

Toutefois, cette dernière imposera ses propres normes et exigences en matière de sécurité, telles qu'une évaluation régulière des risques, ainsi que des capacités de détection et de réaction efficaces.

Par conséquent, les entreprises s'attacheront autant à répondre à ces critères, qu'à se conformer aux normes réglementaires elles-mêmes.

« L'année 2020 a apporté son lot de difficultés et d'enjeux pour bon nombre d'entre nous, confie Pierre-Louis Lussan, Country Manager France et Directeur South-West Europe chez Netwrix.

Ainsi, pour l'année à venir, les entreprises devront affronter les percussions des mesures et des décisions prises lors de la transition numérique, notamment avec le recours massif au télétravail, qui a contribué indéniablement à augmenter les risques de cybersécurité.

Il est donc suggéré aux organisations de revoir les principes de la sécurité afin de veiller à ce que les données sensibles soient bien protégées, qu'elles ne soient pas surexposées et que la gestion des accès privilégiés soit réglementée - voire évitée - si elle n'est pas justifiée. »

### **[À propos Netwrix](#)**