Une Erreur à 1 Million de Dollars:

Comment protéger son entreprise des risques quand les employés travaillent à distance.

FUDO SECURITY

Pour un travail d'équipe efficace, il n'est pas nécessaire que tout le monde soit au bureau. Le principe du travail à distance a été testé pour la première fois par les plus grandes entreprises du monde. En 2018,Jack Dorsey, le responsable de Twitter, a suggéré à ses employés d'essayer de travailler à domicile. Une expérience qui à ce moment-là a montré d'excellents résultats: **les équipes ont pu considérablement l'efficacité de leur travail.**

Depuis mars 2020, Twitter a sous loué certains de ses bureaux et le principe du télétravail est devenu un élément de la culture de l'entreprise.

La pandémie du COVID-19 a accéléré la transition de nombreuses entreprises (spécialement dans le domaine du IT) pour permettre aux employés de travailler en partie à distance.

Pendant une pandémie, cette approche contribue à réduire les risques de contaminations au sein de l'entreprise, mais également de prendre soin de ses employés et de réduire les couts liés à la maintenance des locaux.

LE SAVIEZ-VOUS...

Un sondage réalisé par le cabinet de conseil Gartner montre que de nombreuses grandes entreprises sont déterminées à laisser les travailleurs chez eux après la pandémie, écrit American Forbes. Des analystes ont interrogé 317 directeurs financiers dans des entreprises dont le chiffre d'affaires annuel varie de 500 millions de dollars à 50 milliards de dollars et employant jusqu'à 100 000 personnes. **75% d'entre eux ont approuvé l'idée de transférer une partie de leurs employés en travail à distance.** De plus, les données nous indiquent que 17% des dirigeants de haut niveau prévoient de garder 20% de leur personnel en travail à distance. Il convient également de noter que 4% des managers aiment que 50% de leur personnel travaille à domicile.

1 https://www.gartner.com/en/newsroom/press-releases/2020-04-03-gartner-cfo-surey-reveals-74-percent-of-organizations--to-shift-some-employees-to-remote-work-permanently2

Cependant, cette approche comporte également d'énormes risques que l'entreprise et ses dirigeants ne peuvent ignorer.

La direction de Twitter a identifié les deux problèmes principaux du "travail à distance”:

Des lacunes dans la sécurité de la connexion au réseau de l’entreprise.

L’analyse précise de la productivité des employés.

Le 15 juillet 2020 est devenu une vraie «Journée noire» pour Twitter. Le service de microblogging a plongé de 3,2% après des échanges majeurs. **La raison principale: une attaque de hacker,** qui a affecté les comptes des plus grands hommes d'affaires, célébrités et de grandes entreprises en général. A partir des comptes d'Obama et d'Elon Musk par exemple, les abonnés ont commencé à recevoir des messages avec un appel à envoyer des bitcoins.

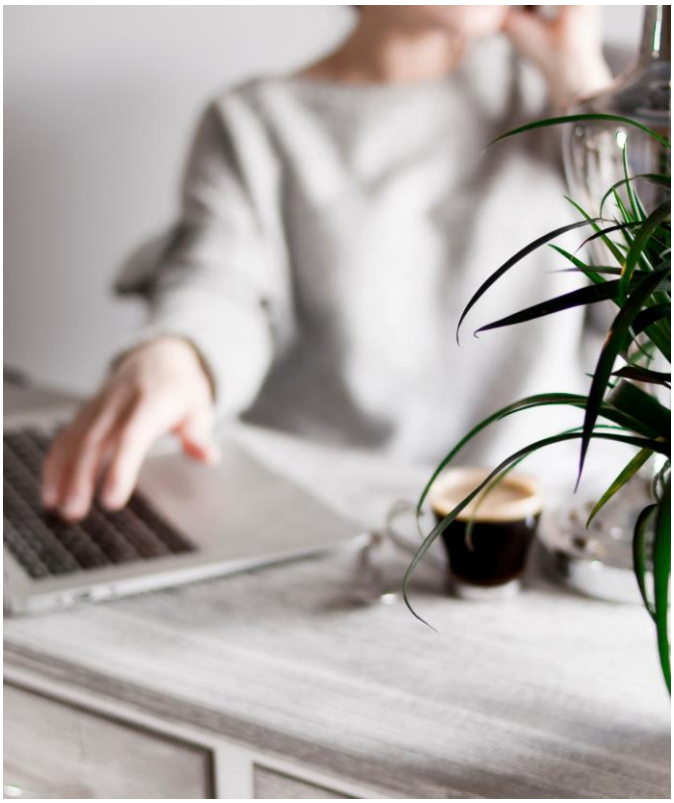
Les employés de Twitter étaient automatiquement déconnectés de leurs comptes, et beaucoup n'ont pas pu se connecter pour discuter avec des collègues pour essayer de résoudre la situation.

Un coup dur pour la réputation de l'entreprise et ses profits, n'est-ce pas? Comment cela a-t-il pu arriver dans une société apparemment protégée de manière fiable?

Les pirates ont utilisé une attaque massive en utilisant une technique d'ingénierie sociale. Imaginez, une note qui provient prétendument d'un gestionnaire avec une demande pour fournir certaines informations confidentielles. Si vous êtes au bureau, il est facile de vérifier avec votre collègue la véracité du document. Cependant, lorsqu'un employé travaille à domicile, qu'il dispose d'une connexion Internet non sécurisée, qu'il y a des animaux de compagnie et des enfants à surveiller, alors la vigilance s'émousse. Ce genre d'environnement est bien sur **propice pour**

Pour de nombreuses entreprises, la transition vers le travail vers des «bureaux à domicile» fut une découverte. Il n'a pas été possible d'assurer correctement le niveau requis de sécurité lorsque les employés se sont mis à travailler à distance.

En conséquence, la plupart des systèmes d'accès à distance dans une entreprise se font par le matériel ou par une solution logicielle du côté entreprise et VPN du côté des utilisateurs. Ceux-ci peuvent être à la fois des produits commerciaux et gratuits, par exemple OpenVPN. Dans ce cas, à la maison ce sont des ordinateurs fixes et des ordinateurs portables qui sont utilisés comme postes de travail. Et c'est là où la protection de connexions à distance se joue !



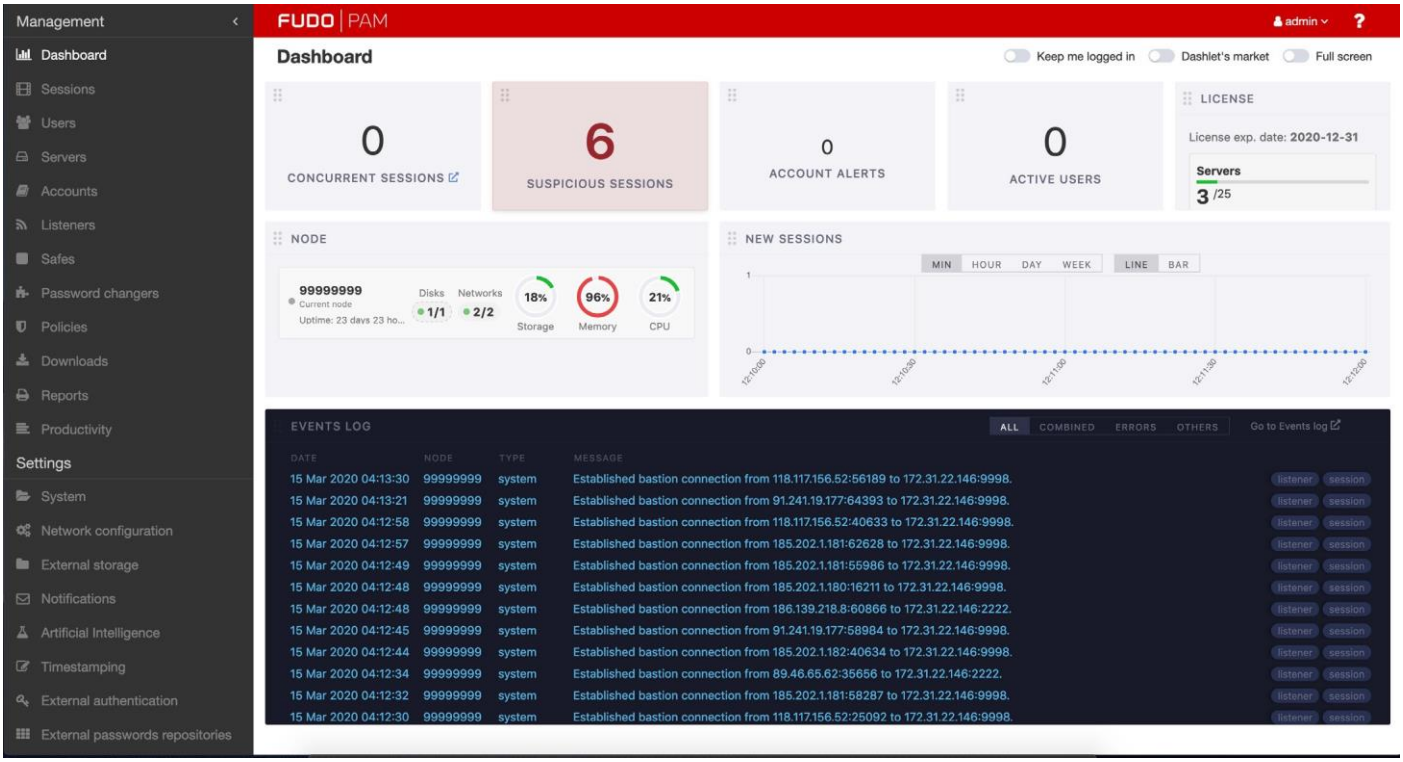
Naturellement, une faible protection conduit à une forte augmentation d'incidents et une augmentation du nombre de hacks.

> **Au cours des six derniers mois, le nombre de cyberattaques a augmenté de 150%.**

Au cours des six derniers mois, le nombre de cyberattaques a augmenté de 150%. Par exemple, si au début de l'année le nombre d'attaques sur le « bureau distant » était d'un peu moins de **60,000 par jour** autour du monde, pendant la pandémie, le nombre d'attaques était passé à – **plus de 100.000 par jour !**[2]

C'est donc un défi pour les gérants et pour les responsables des départements sécurité IT de l'entreprise. Il est en effet nécessaire de choisir une solution qui fournit une protection fiable contre les cyber-fraudeurs, et en même temps, qui offre une mise en œuvre qui ne prendra pas beaucoup de temps et sera financièrement abordable.

2 https://www.esetnod32.ru/company/press/center/eset-vo--vtorom-kvartale-kolichestvo-atak-na-rdp-vyroslo-v-dva-raza/



Fudo PAM est une solution prête à l'emploi, avec un matériel ou logiciel qui peut être déployé sur le réseau du client dans un délai de quelques heures sans exiger d'achat supplémentaire de licences.

Pour la sécurité de la connexion, Fudo PAM propose au client l'utilisation d'une option, avec un **facteur d'authentication.**

Par exemple, cela peut être un code généré sur votre téléphone par l'application gratuite Google Authenticator. L'utilisateur entre alors son nom d'utilisateur et mot de passe, puis le code lui est donné par l'application.

Ainsi, même si un hacker a volé le mot de passe de connexion d'un utilisateur, sans accès à son téléphone il ne pourra pas se connecter aux ressources.

Cette fonctionnalité est gratuite pour les utilisateurs de Fudo PAM et prend en charge les deux Google Authenticator gratuits ainsi que l'application Microsoft Authenticator mais également les produits commerciaux comme Vasco, RSA, Cisco DUO et d'autres.

Les systèmes Microsoft Active Directory et LDAP sont pris en charge. Il est possible de combiner l'accès des systèmes d'entreprise avec diverses méthodes à deux facteurs d'authentification. **Il n'y a pas de nécessité d'installer un quelconque logiciel sur les serveurs et sur les postes de travail.**

Pour fournir en permanence, une évaluation de la performance des employés en télétravail, Fudo PAM inclut, **un Module d'analyse de l'efficacité.** Ce module analyse l'activité de l'employé à distance: **l'activité d'utilisation de la souris et du clavier, la quantité d'informations s'affiche à l'écran.**

> **Si une analyse détaillée ou un "débriefing" est requis, les sessions à distance peuvent être enregistrées sous forme de fichier vidéo.**

Ces informations sont collectées, analysées par le système Fudo. Ensuite, sous forme de graphiques et de rapports, il peut être présenté aux responsables de l'entreprise: rapports par départements, groupes, pour un salarié. **Si une analyse détaillée ou un «débriefing» est nécessaire, les sessions à distance peuvent être enregistrées sous forme de fichier vidéo.** Vous pouvez toujours garder et enregistrer une situation controversée.

En même temps, l'enregistrement est effectué uniquement dans le cadre de session de travail, donc si un employé utilise un ordinateur à la maison pour le travail, l'intimité de sa vie personnelle n'en souffrira pas.

Comme une invitation à la sécurité, il y a une possibilité d'améliorer encore la protection. Le système Fudo inclut une analyse biométrique, comme une écriture numérique, pour protéger l'utilisateur d'un vol et d'une mauvaise utilisation des informations d'identification.

Grâce à cette fonction, le système Fudo vous permet d'avertir un employé de l'état de la sécurité ou même de bloquer l'accès automatiquement si quelqu'un utilise son mot de passe.
Un étranger aura une écriture qui sera différente de celle d'un de vos employés

Toutes ces fonctionnalités permettent aux entreprises de tout niveau d'ajouter rapidement des commandes essentielles pour leur collaborateur avec un système d'accès à distance.

Cette technologie améliore la sécurité et permet à l'entreprise de surveiller la performance de ses employés. Il convient de noter la facilité de mise en place des produits Fudo.

L'offre Fudo Security est unique et personnalisable selon des modèles de tarification abordable et pour toutes les situations. Vous n'avez pas à vous soucier du nombre d'utilisateurs qui n'est pas limité. Par exemple, la connexion de 100 utilisateurs à 1 serveur ne nécessitera l'achat d'une seule licence Fudo. Et toutes les options présentées ci-dessus peuvent être incluses dans cette licence.

fudosecurity.com

Accès à distance Sécurisés

Déployable en un seul jour.

+33(0)1 40 86 04 26

contact@ipsteel.com
https://www.ipsteel.com/

DEMANDE D'ESSAI

DEMANDE DE DEVIS

FUDO SECURITY