Mobilité professionnelle : Les nouveaux risques

PSM Magazine Novembre N°222

dossier MOBILITÉ PROFESSIONNELLE : LES NOUVEAUX RISQUES

© Thinkstock

Les entreprises multisites doivent choisir des systèmes de contrôle d'accès qui leur permettent d'accorder, si nécessaire, des droits temporaires à leurs collaborateurs. Puis de supprimer ces droits de manière très simple.

Identifier les personnes et les objets

La mobilité génère des risques supplémentaires. Nous nous déplaçons plus. Et nos outils de travail aussi. Il faut donc être certain que l'utilisateur d'un périphérique mobile soit le bon. Il faut aussi être capable de vérifier que l'objet qui permet de s'assurer de son identité – pour entrer sur un site ou accéder à ses outils informatiques – soit autant que possible inviolable. Mais comment faire ? Quelles solutions retenir ? Comment réduire les risques ? Quelles pratiques adoptées ? Quel rôle assigné aux salariés ?....

La mobilité commence au sein même de l'entreprise

« Dans le cadre de notre activité, nous sommes confrontés à des entreprises qui parfois ont à gérer 2500 mini-déménagements par an. Ces opérations comprennent la réorganisations des espaces, des bureaux, le déplacement d'unités... À chaque fois, les responsables de la sécurité informatique et de la sûreté (DSI et DS) doivent reconfigurer leur contrôle d'accès et les droits associés à chaque badge ou carte, explique Pierre-Antoine Larrera de Morel, directeur commercial chez STid. Cela pose des problèmes techniques et de sécurité évidents pour l'entreprise. Elle doit donc se doter d'un système de contrôle d'accès qui soit le plus souple possible. Afin qu'il puisse évoluer facilement et s'adapter à la nouvelle configuration du site et aux nouveaux droits d'accès donnés à certains collaborateurs ».

Or, souvent faute d'anticipation, faute d'avoir anticiper ce type de problématique, les entreprises sont découragées par la complexité de la remise à niveau de leur système de contrôle d'accès et le coût induit. Elles lâchent donc l'affaire et se retrouve avec un système bancal et faillible.

3 questions à

MARC MENESES

Directeur commercial groupe Insiders

Les entreprises sont-elles conscientes des risques inhérents à la mobilité de leurs salariés et des outils informatiques qu'elles leur fournissent ou que les collaborateurs utilisent à titre privé dans le cadre de leurs missions ? Quand se tournent-elles vers vous ? En amont, à titre préventif ou à titre curatif ?

Les sociétés font le nécessaire pour protéger les outils nomades. En revanche, ce sont les salariés qui lors d'une utilisation dans la sphère privée «oublient» les risques encourus, en utilisant les applications non prévues par la charte de l'entreprise ou en désactivant certaines protections. De même, des connexions intempestives à des Wi-Fi ouverts, sans tenir des recommandations et outils spécifiques, fragilisent les protections et peuvent faciliter le travail de pirate informatique. Si la NSA a développé la quintessence de ce qui peut être en matière de piratage, des hackers privés peuvent développer des techniques plus ciblées (quelques individus), plus rudimentaires, mais pas moins efficaces. Trop souvent, en cas d'accident, on ne peut que constater les dégâts et faire des préconisations qui sont très souvent déjà prévues par les services DSI/RSSI. Le cas le plus typique est l'utilisation des tablettes. Elle peut être utilisée par les salarié, en réunion, en déplacement, puis par ses enfants. Par maladresse, ils peuvent alors installer un virus ou rooter le système, qui fragilise les protections mises en place par la DSI, et de là toute l'entreprise. Ainsi le fait de prêter son outil à un proche est un facteur de risque.
Cependant certains groupes ou entités font appels à Insiders pour sensibiliser l'ensemble des personnels y compris le comité de direction sur les risques de piratage, de fuites, de non-respect de la charte d'utilisation ou d'utilisation d'outils personnels dans le cadre professionnels. Insiders réalise des démonstrations de ce que risque un manager lors d'un déplacement s'il ne pas respecter les consignes éditées par son entreprise. Et pas uniquement à l'étranger...

Les problématiques sécuritaires de la mobilité sont-elles du seul ressort du DSI ou concernent-elles aussi le directeur sûreté-sécurité ? Ces derniers en sont-ils conscients ?

La fuite d'information concerne tout le monde, le DSS et le DSI ont en conscience. Il ne faut pas opposer l'un et l'autre. Les sociétés les mieux protégés sont celles où la synergie de ces deux services est optimale. Les problématiques et des solutions sont prises en commun. L'un maîtrise les risques informatiques, l'autre les risques humains. Trop souvent l'investissement nécessaire porte sur les systèmes informatiques. La faille aujourd'hui est l'humain. Le comportement du salarié dans sa prise de conscience qu'il détient une information et qu'il doit la protéger permet de réduire les fuites d'information. «j'utilise les bons outils, je communique selon les règles éditées par la DSI, j'écoute les recommandations de mon DSS» sont des garants de la conservation de l'information. Cela s'applique de l'employé au DG. Etre issus d'une grande école ne protège pas !

Quelles questions doivent se poser les entreprises qui sont confrontées à ce type d'enjeu ? Quels conseils leur donneriez-vous ?

Les DSI et les DSS se posent les bonnes questions : Où sont les failles ? Mon système est-il bien protégé en fonction de sa mission ? Mes données sont-elles bien conservées et protégées ? Les investissements sont généralement faits, car la direction générale en a conscience et le travail d'information du DSI porte enfin ces fruits. Le fait d'investir des milliers d'Euros dans les systèmes informatiques est nécessaire, trop souvent l'entreprise s'arrête là «j'ai investi 1 million euros dans cette solution informatique». En revanche ce qui manque s'est de sensibiliser l'ensemble des salariés. L'attaque d'entreprise à entreprise est une réalité bien plus importante et plus nombreuse que les grandes affaires sorties dans la presse.
Cela touche tous les secteurs et toutes les tailles d'entreprises. L'espionnage économique, l'escroquerie ou le chantage passent très souvent par un individu, qui par son comportement non adéquat, ouvre une porte vers les serveurs de l'entreprise. Car chacun encore une fois détient une part de savoir et de valeur ajoutée de son entreprise. Il faut donc sensibiliser les équipes. Le DSS en a conscience, parfois les moyens lui manquent...

■ *Gérer les identifiants ? Oui. Mais comment ?*

«Les nouveaux outils communicants ouvrent de réelles perspectives quant à la gestion des accès et de l'identité numérique des collaborateurs. On voit bien le principe : permettre à un support périphérique de générer un code temporaire ou non qui donne accès à un bâtiment ou à des données stockées sur un support informatique, explique Yves Ackermann. Or, si le principe est simple, c'est la gestion des identifiants – leur création, leur codage et leur validation – qui est plus complexe. Prenons l'exemple d'un smartphone utilisé pour donner accès à un local via un échange d'informations entre le téléphone et le lecteur. Cela pose plusieurs problèmes : être certain que l'utilisateur du téléphone est la personne habilitée à la faire, prouver la présence du téléphone, etc.» Cela suppose de la part de l'entreprise la définition de nouvelles procédures quant à la création de l'identifiant et de qui en a le droit. Cela suppose aussi qu'on est certain que le support qu'on utilise pour communiquer avec l'infrastructure de contrôle d'accès est sûr. Or, ces procédures – dans la plupart des entreprises – n'existent pas.

La mobilité des collaborateurs implique donc une nouvelle forme de gestion des identifiants. «Trop souvent, cela se fait encore de manière locale, par régions ou par pays, regrette l'expert d'HID. Malheureusement, on génère ainsi des sous-niveaux de données, de codes qui ne sont pas gérés de manière centralisée et qui augmentent considérablement le volume des données à exploiter».

■ *Partager les droits sans partager les secrets*

«La gestion des droits d'accès doit se faire de manière centralisée. En effet, quand on accorde des droits d'accès à un collaborateur on accepte de partager des secrets via le support qui lui donne accès au site ou à l'infrastructure informatique, rappelle Pierre-Antoine Larrera de Morel. Se pose alors la question de savoir comment on lit le badge comment on identifie ce qu'il contient. Dans ce cas de figure, on comprend bien qu'on autorise le site sur lequel se présente le collaborateur à lire son badge. On doit donc s'assurer de permettre cette lecture sans compromettre la sécurité. Cela requiert la mise en place d'une gestion segmentée de la sécu- ● ● ●

● ● ● rité physique et informatique qui permet de partager les droits sans partager les secrets ».
Pour Yves Ackermann, « la mobilité requiert une gestion globale des identifiants. Il faut tous les lister, quel que soit le support. Il faut aussi détailler le processus de vie des différents identifiants : qui peut autoriser leur création ? Leur suppression ? Selon quels principes ? Il faut privilégier des technologies évolutives, compatibles avec les cartes et les smartphones pour quelles puissent gérer les informations sur les cartes et les communications entre les téléphones et les systèmes centraux ».

■ *Simplifier mais pas trop*

Le maintien d'un bon niveau de sécurité passe donc par la simplification. Le directeur commercial de STid le confirme : « Simplifier ne veut pas dire laisser tout faire à un système qui gère tout en dehors de vous, type Cloud. Car quand on veut reprendre la main, cela s'avère souvent difficile. Simplifier veut se doter d'outils qui permettent de gérer la sécurité et l'identification des personnes et des outils mobiles de manière simple. Les grandes entreprises le comprennent. Si elles délèguent encore, par exemple, la production des badges, elles gardent la main sur la création des droits et des données et leur gestion. Elles sont dans une certaine forme de délégation interne avec une véritable centralisation des données sensibles ». Mais il faut disposer des bons outils. « Les entreprises pour être sûres que leur politique sécurité soit respecter au niveau local doivent avoir opté un système central qui leur permette de s'affranchir d'un certains nombre d'infrastructures locales dédiées. Elles pourront ainsi limiter les failles dans leur système, conseille Yves Ackermann. Mais cela ne peu se faire que si les identifiants de l'entreprise utilisent les standards de programmation et de communication. Pour assurer la sécurité de la mobilité, il faut être compatible... ».

■ *Un rapprochement nécessaire en DSI et DS*

« Ces nouveaux paradigmes qui s'imposent à l'entreprise impliquent une parfaite collaboration entre la direction informatique et la direction sûreté-sécurité. Chacune ne doit pas croire que l'autre va lui « voler » une partie de ses prérogatives, explique Pierre-Antoine Larrera de Morel.
DSI et directeur sécurité/sûreté doivent collaborer. Si chacun campe sur ses positions cela se fera au détriment de la sécurité/sûreté de l'entreprise. La DSI a un rôle de définition de la stratégie sécuritaire liée à la mobilité. Le directeur sûreté/sécurité doit, quant à lui, jouer le rôle d'animateur par rapport aux procédures définies. Il est en première ligne pour porter le message de la DSI auprès des collaborateurs qui sont souvent le maillon faible de la sécurité ». ■

PIERRE-ANTOINE LARRERA DE MOREL
Directeur commercial chez Stid

« LES ENTREPRISES DOIVENT ANTICIPER LES PROBLÉMATIQUES LIÉES À LA MOBILITÉ »

« Il est certain que la mobilité – des personnes et des outils – va poser de plus en plus de défis au monde de l'entreprise. Pour les gérer de la manière la plus efficace et la moins perturbante pour leur activité, elles doivent anticiper ces questions et se former aux nouvelles procédures, aux nouvelles technologies, aux nouvelles compétences de chacun. Actuellement, les grands-comptes qui l'ont compris acquièrent des compétences qui leur permettront très vite de déployer des nouvelles solutions de sécurité pour gérer droits d'accès, identification... Du côté des fabricants, il faut réfléchir au développement de solutions qui n'existent pas encore et qui permettront, par exemple, de greffer sur un smartphone ou une tablette une application réellement sécurisée pour faire de ces outils de nouveaux supports d'identification. »