La sécurité du poste de travail au sein des collectivités territoriales

Virus, failles logicielles, intrusions, perte d'informations sont autant de problématiques auxquelles sont confrontées les administrations et les collectivités territoriales. L'informatique est devenue un élément stratégique pour une large majorité de collectivités. Ainsi les indisponibilités liées à ces différentes nuisances sont de moins en moins tolérées par les utilisateurs et les citoyens, d'autant plus qu'elles ont un impact direct en termes de coûts et de productivité.

Les collectivités territoriales sont des structures administratives françaises, distinctes de l'administration de l'état, qui doivent prendre en charge les intérêts de la population d'un territoire précis. Des fonctions d'état civil et électorales aux actions sociales, à l'éducation sans oublier l'aménagement du territoire, la protection des citoyens et le financement des biens de l'état, les collectivités doivent faire face à de nombreux dossiers sensibles.

Pour toutes ces raisons les collectivités sont devenues des cibles de choix pour les pirates informatiques qui constituent aujourd'hui de véritables organisations criminelles. Falsification de documents administratifs, récupération d'informations confidentielles ou juste simple nuisance, les motifs d'attaque sont nombreux. Les budgets alloués à la sécurité de l'information restent pourtant difficiles à identifier tant les besoins sont variés et de plus en plus importants. Chaque collectivité reste autonome dans ce choix stratégique de la sécurité informatique, et plus qu'ailleurs les responsables de la sécurité du système d'information (RSSI) doivent faire face au manque de collaboration du personnel et aux restrictions budgétaires.
Si beaucoup de collectivités sont encore dans l'incapacité de fournir une Politique de Sécurité de l'Information qui prendrait en compte tous les risques, tous s'accordent à dire qu'avec l'ouverture du SI et la mobilité des utilisateurs, la sécurisation du poste de travail est devenue un enjeu majeur.

Le HIPS – Un des nouveaux enjeux de la sécurité

La sécurité du poste de travail s'est longtemps limitée à l'utilisation d'un antivirus voire d'un firewall. Aujourd'hui cela ne suffit plus : les systèmes antivirus basés sur les signatures ne sont pas assez réactifs face aux nouvelles menaces. Ils ne permettent pas de se protéger contre les attaques zero day (non identifiées) et les attaques ciblées.
Les pirates s'adaptent et utilisent des variantes des virus qui ne sont pas reconnues. Les logiciels bureautiques, de plus en plus complexes, font l'objet de failles de sécurité exploitables. Dernièrement le ver Conficker et les attaques sur le Reader d'Adobe ont causé un grand nombre d'interruptions de service au sein des entreprises et des organismes d'état.
Au Royaume Uni, une infection par Conficker a coûté 2,5 millions de dollars à la Mairie de Manchester (pertes et les coûts de remise en état de son système d'information).
Devant ce constat et l'impuissance des directions informatiques, une solution semble s'imposer : le HIPS (Host Intrusion Prevention System ou système de prévention des intrusions basés sur des hôtes).

Cette technologie de défense automatique se base sur un mécanisme de détection intelligent. Ainsi, sans base de signature mais grâce à la reconnaissance de caractéristiques génériques propres à certains types d'attaques, un HIPS va détecter tout comportement anormal sur le poste de travail et agir instantanément pour en bloquer les effets néfastes. Que la nuisance vise le comportement du système ou celui des processus, le HIPS va remédier à l'attaque non détectée par l'antivirus en inhibant l'action malicieuse.

Cette technologie réactive a déjà fait ses preuves dans des domaines comme la défense ou l'industrie. On la retrouve en premier lieu sur les ordinateurs portables plus sensibles aux attaques car plus amenés à se connecter à des réseaux non ou mal maîtrisés.
Cependant, aujourd'hui les menaces sont partout. Un simple site web visité par un utilisateur peut corrompre son poste et mettre en péril tout le système d'information et les données qu'il contient. Or, une collectivité territoriale, de part ses obligations envers la CNIL et envers les citoyens, ne peut pas se permettre de tels risques.

Des solutions logicielles adaptées pour une protection efficace des PC

Pour aider les collectivités à adresser l'ensemble des menaces liées au poste de travail, il existe des solutions logicielles permettant de protéger le parc micro-informatique de manière optimale.

Utilisant le HIPS, ces solutions protègent automatiquement le système d'exploitation et les applications en cours d'exécution à l'aide de mécanismes de détection et de blocage des anomalies. Ces protections automatiques permettent par exemple de bloquer les attaques par débordement de mémoire (buffer overflow), l'espionnage des frappes au clavier (keylogging) ou les tentatives de corruption des processus en mémoire, mécanismes bien souvent utilisés par les cybercriminels pour prendre possession des données administratives confidentielles.
Par ailleurs, la protection du système d'exploitation, la sécurisation des données mais également le contrôle des utilisateurs sont des problématiques incontestablement liées. Certaines solutions intègrent donc des couches de protection additionnelles afin de contrôler l'usage des postes.

Outre les attaques ciblées, le téléchargement d'une application compromise, l'utilisation d'une clé USB infectée ou une connexion internet non-sécurisée sont bien souvent le vecteur d'entrée de nouvelles attaques. Les directions informatiques doivent donc s'assurer que le poste de travail est utilisé de manière conforme. Des fonctionnalités de contrôle (des périphériques externes, des applications, d'accès au réseau…) peuvent alors s'ajouter à l'HIPS pour renforcer la protection du poste client, assurer l'intégralité des données qu'il contient et garantir sa continuité de fonctionnement.

Accompagnant des conseils généraux, municipalités et autres collectivités territoriales dans leurs projets de sécurisation du poste de travail depuis plusieurs années, SkyRecon Systems connait parfaitement les problématiques spécifiques auxquelles ces structures sont confrontées et leur apporte une solution adaptée.

À propos de SkyRecon Systems

SkyRecon Systems est un éditeur de logiciel français, précurseur de la sécurité comportementale, proactive et intégrée du poste de travail. Abordant la sécurité sous un angle complémentaire aux technologies antivirus, sa solution logicielle StormShield délivre en un agent unique une protection complète du système, des applications et des données, sur tout PC mobile ou fixe. StormShield permet la mise en application et le contrôle d'une politique de sécurité dynamique comprenant notamment la détection contre les intrusions (HIPS), le firewall, le contrôle des applications, le contrôle de périphériques amovibles, la sécurité des réseaux sans fil et le contrôle d'accès réseau (NAC). SkyRecon Systems a développé des partenariats technologiques forts avec Microsoft, Juniper, VMWare, Intel et HP. Créée en 2003, la société a été distinguée par de nombreuses récompenses internationales et a intégré le prestigieux Magic Quadrant 2009 du Gartner consacré à la protection du poste de travail. La société accompagne ses clients en Europe et aux Etats-Unis depuis ses bureaux de Paris et San Jose. Pour plus d'informations : www.skyrecon.com.