Un routeur recyclé se reconnecte automatiquement à son ancien réseau

- Informatique - Sécurité Informatique -

Date de mise en ligne : mardi 21 octobre 2008

C'est la mésaventure qui est arrivée à une administration anglaise, avec un routeur envoyé au recyclage. Ce type d'équipement contient des données sensibles trop souvent oubliées.

Lorsqu'une entreprise se débarrasse de tout ou partie de son parc informatique, les disques durs ne sont pas les seuls à pouvoir se révéler trop bavards. La société britannique Random Storm, spécialisée dans la sécurité, vient d'en faire l'étonnante constatation après avoir acheté sur eBay un routeur VPN (1) d'occasion de marque Cisco. Une fois connecté à Internet, l'appareil a donné automatiquement un accès direct à l'intranet sécurisé du... District métropolitain de Kirklees, dans le Yorkshire, au Royaume-Uni !

Des clés d'accès très sensibles

« Ce cas illustre une réalité méconnue de beaucoup d'entreprises, et en particulier des PME : les disques durs des PC de bureau, des portables et des serveurs ne sont pas les seuls équipements contenant des informations critiques. Les équipements réseaux comme les routeurs, les box ADSL et les firewalls sont des équipements de connectivité qui peuvent contenir des clés donnant un accès direct à des informations très confidentielles ou révéler des failles de sécurité exploitables par des hackers », explique Sylvain Roger, consultant en sécurité chez Solucom.

Les routeurs enregistrent en général sur une mémoire flash les paramétrages (identifiants, mots de passe, adresses IP, etc.) mis en place par les administrateurs réseaux. Ces données ne sont pas effacées par les prestataires chargés de recycler le matériel en fin de vie. Mise en cause, la société britannique qui a revendu le routeur du district de Kirklees sur eBay a ainsi expliqué que la gestion des données de configuration des équipements réseaux restait sous l'entière responsabilité de ses clients.

En France, les sociétés de recyclage les plus sérieuses ne prennent pas non plus en charge de genre de manipulation. « Nous avons une technologie très efficace, baptisée Blanco, qui efface les contenus des disques durs, mais nous n'effaçons pas les configurations des équipements réseaux. Il y a une multitude de matériels différents, et proposer ce service serait un investissement relativement coûteux. Or, nous n'avons pas de demande pour l'instant », avance Sylvain Couthier, président d'ATF, une société spécialisée dans la valorisation des équipements informatiques en fin de vie qui travaille essentiellement pour des grands comptes.

L'entreprise doit effacer les configurations

« Effacer ce type de données reste une prérogative de l'entreprise. Je ne crois pas que c'est un service qui va se développer, car les volumes de matériels à traiter sont très faibles », confirme Jean-François Audenard, responsable du développement des services de sécurité d'Orange Business Services. Selon lui, les équipements réseaux les plus sensibles sont les routeurs VPN qui utilisent des clés partagées identiques sur chaque routeur.

« La plupart des PME se contentent de clés PSK - Pre-Shared Key - et n'effectuent pas d'authentification spécifique du matériel. C'est le cas du routeur retrouvé sur eBay », déclare-t-il. Effacer les données de routeurs contenant de telles informations est donc absolument nécessaire. La plupart des équipements contiennent une fonction de « reset matériel », qui restaure les paramètres d'usine en effaçant au passage toute la configuration mise en place par l'entreprise.

Comme pour les disques durs reformatés, il demeure toujours un risque que des pirates essaient de scanner la

mémoire flash pour retrouver des informations (comme il existe des logiciels pour récupérer les photos effacées par mégarde sur des cartes mémoire), mais cela demande des moyens importants. « Tout dépend du niveau de risques. Pour les secteurs et les applications sensibles, comme la finance ou la Défense, il vaudra mieux procéder à une destruction physique des équipements sensibles en fin de vie », illustre Sylvain Roger.

Activer les verrous des nouveaux matériels

« Pour 95 % des entreprises, la réinitialisation du matériel est amplement suffisante », confirme Jean-François Audenard. Selon lui, effacer les données des équipements qui sortent de l'entreprise est une procédure qui doit être systématiquement mise en place dans les services chargés de gérer les immobilisations.

Et puis de la même manière qu'il est important d'effacer les données en sortie, il faut penser à activer les verrous lors de la réception d'un nouveau matériel. « Dans les PME, combien de configurations de routeurs sont accessibles en utilisant simplement le login et le mot de passe fournis par défaut par le constructeur ? », s'interroge-t-il.

(1) Virtual Private Network, ou réseau privé virtuel en français fournit aux utilisateurs des accès réseaux sécurisés en mettant en oeuvre des communications IP chiffrées de bout en bout (on parle aussi de « tunnels » VPN).

Post-scriptum :

http://www.01net.com/editorial/3938...