Microsoft TechDays : Bernard Ourghanlian, « La situation en matière de sécurité n'a jamais été aussi grave qu'aujourd'hui »

Silicon.fr : ***Microsoft fête les 10 ans de l'informatique de confiance. Pouvez-vous nous dresser un bilan de la sécurité informatique aujourd'hui ?***

Depuis le lancement de cette initiative, beaucoup de choses ont changé. En particulier l'environnement social de l'informatique. Il ne s'agit plus simplement de la faire marcher, c'est toute notre vie sociétale qui en dépend. C'est le phénomène irrépressible et majeur de la consumérisation de l'informatique, par lequel nous assistons à l'apport d'usages de la maison dans l'entreprise, et au floutage des frontières entre les mondes professionnel et personnel. Ainsi que de temps en temps à de petites dérives avec les métiers en entreprise qui achètent des services informatiques et des solutions en dehors de la DSI parce ce que celle-ci est trop lente à réagir.

Ce sont des phénomènes nouveaux et qui ont des conséquences très importantes sur la façon dont on peut imaginer sécuriser le système d'information au sens large. La notion de périmètre du système d'information (SI) est en train de disparaître. Les systèmes sont plus ouverts, ainsi que les usages des collaborateurs de l'entreprise. Les choses changent, et dans le même temps les menaces évoluent.

Silicon.fr : ***Elles évoluent, mais sont-elles plus dangereuses ?***

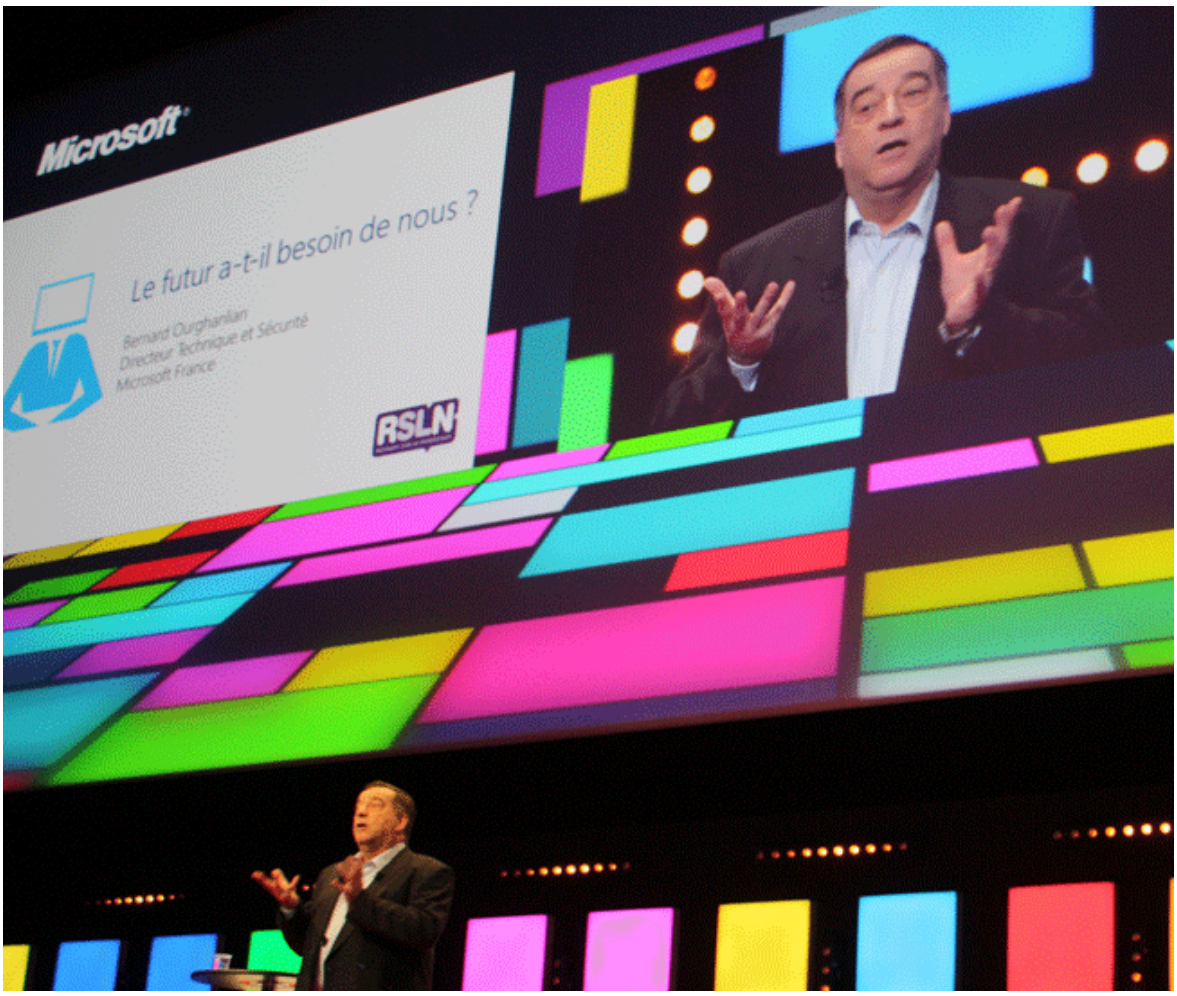
Paradoxalement, la situation en matière de sécurité n'a jamais été aussi grave qu'aujourd'hui. Contrairement à ce qui s'est passé avant que nous lancions l'initiative de l'informatique de confiance, les menaces qui ont défrayé la chronique étaient des phénomènes visibles, qui ont infesté plusieurs millions d'ordinateurs sur la planète. Aujourd'hui, les attaques sont plus ciblées, plus déterminées, qui aboutissent à ce que l'on appelle APT (*Advance Persistent Threats*) avec des conséquences dramatiques, dont un certain nombre ne sont pas publiques. Ces attaques généralement perdurent depuis longtemps, parfois depuis plusieurs années, avec des attaquants qui souvent ne pratiquent pas des techniques très sophistiquées, mais par contre opèrent de manière industrielle, avec des employés, et qui ne font que cela. Leurs objectifs portent sur le vol d'informations, de secrets et de propriétés industrielles, d'informations d'ordre géostratégique pour les administrations et les gouvernements. Des vols pratiqués avec la volonté de les monétiser, voire avec la complicité bienveillante et probablement le financement d'États, ce que nous ne pouvons cependant pas affirmer de manière péremptoire.

Quand ce genre de chose arrive. Les entreprises sont alors désemparées, car personne n'a pu imaginer ni planifier que le SI ne vous appartient plus ! Les entreprises n'ont pas de plan d'action et se retrouvent dans une situation particulièrement dramatique. C'est un sujet qui préoccupe beaucoup de nos clients et sur lequel Microsoft a travaillé. La situation ne peut pas durer.

Silicon.fr : ***Nous avons parfois l'impression que la sécurité s'est banalisée.***

Beaucoup d'entités ont quelque peu baissé la garde, parce que l'architecture du SI n'est plus adaptée. Pendant des années, les entreprises se sont réfugiées derrière les pare-feux, en estimant, comme dans un château fort, que les méchants sont à l'extérieur et les bons à l'intérieur. Malheureusement ce mode de fonctionnement est devenu obsolète, à cause de la consumérisation, mais aussi parce que les SI se sont ouverts dans l'objectif de pouvoir échanger des informations. Il est donc normal que des saletés entrent dans le SI, et ce n'est pas forcément grave. À condition que les données critiques soient protégées, que l'on puisse éviter que les logiciels malfaisants nuisent. À cause également et par exemple d'un nombre limité de personnes chargées de l'administration qui disposent de procédures particulières pour accéder au système. Aujourd'hui, dans l'immense majorité des cas, les entreprises sont vulnérables parce que les systèmes ne sont pas mis à jour, le *patch management* est absent, les mots de passe dans l'Active Directory sont soit inexistants soit sur deux caractères, sans politique d'expiration pour les personnes privilégiées, etc.

Nous assistons à une forme de relâchement sur les *« basics »* de la sécurité, et à une fuite en avant des entreprises qui empilent des solutions de sécurité pour créer une usine à gaz qui donne une fausse illusion de la sécurité. C'est la première très grande tendance des menaces. Les attaques sont extrêmement déterminées, durant de longues périodes, au motif de passer inaperçu. L'objectif n'est plus égotique, mais purement financier.



La suite : la sécurité dans le *cloud*, la position stratégique de Microsoft et l'affaire Megaupload.