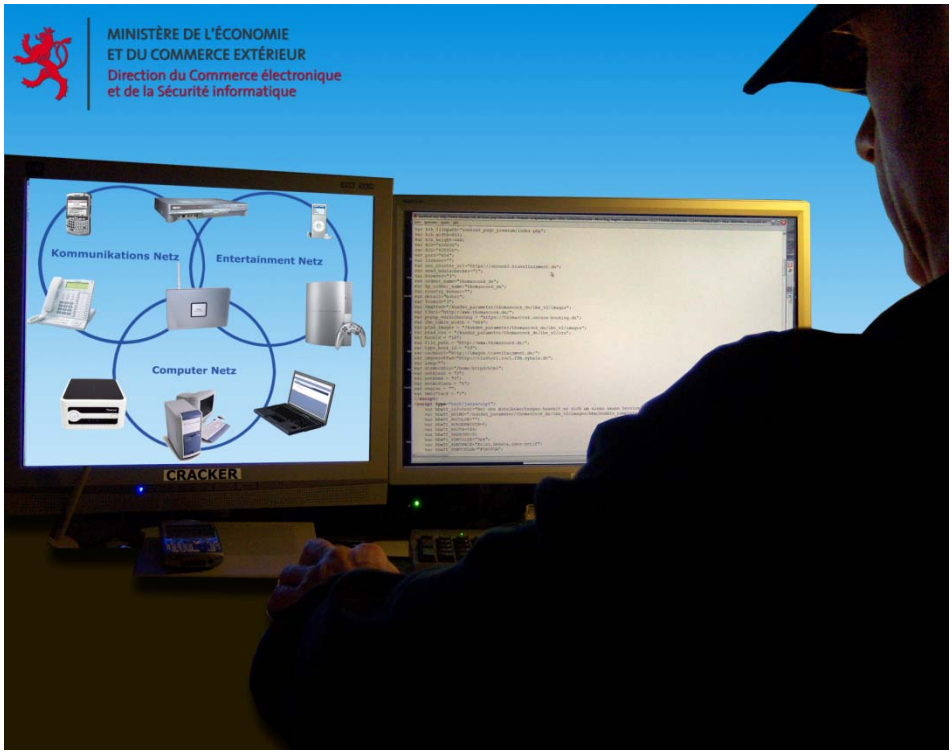
CASES articles
Tirer des enseignements de ses points faibles

« Hackers »
Les acrobates du clavier

Pour plus de sécurité, adoptez les réflexes CASES !

Il est toujours bon de les écouter

Les menaces Internet répertoriées en 2007 atteignaient le chiffre impressionnant de 131 800. Jusqu'à la fin 2008, on a estimé à750 le nombre de nouveaux malwares apparus chaque jour. Le marché est lucratif, car de nombreux systèmes présentent des points faibles. Ce sont bien souvent les hackers qui les détectent et attirent l'attention sur ceux-ci, afin de protéger les systèmes. Pour les entreprises et les scientifiques, il est toujours bon d'accorder une oreille attentive à ces acrobates de l'informatique.



L'Internet a créé un grand nombre de nouvelles perspectives pour les personnes privées et les entreprises et contribue aujourd'hui de façon significative au produit intérieur brut. Les innovations et interconnexions, dont la technologie est toujours plus complexe, ont toutefois également fait augmenter le nombre des vulnérabilités et accentué les conséquences de ceux-ci. La criminalité s'est également introduite dans le marché informatique. Elle s'est adaptée à son développement et les agissements des cybercriminels sont aujourd'hui hautement professionnels et interconnectés. Outre les personnes privées, ce sont en particulier les entreprises et les organisations qui focalisent l'attention des pirates. De nos jours, l'espionnage industriel est devenu courant, même au niveau des moyennes entreprises. Les attaques ciblant l'informatique des entreprises sont rarement sans conséquences. L'éventuel arrêt des systèmes génère souvent très rapidement des préjudices financiers et en termes d'image. Dans tous les cas, des ressources humaines et un investissement en temps sont nécessaires pour analyser les dégâts et y remédier. Les conséquences d'une intrusion par des individus malintentionnés dans des systèmes hospitaliers, de gestion du trafic, de télécommunications ou de distribution électrique par exemple pourraient être catastrophiques.

Le marché informatique est caractérisé par un rythme effréné, les innovations et les possibilités se bousculent. Malheureusement, c'est bien souvent la sécurité qui en souffre le plus. En particulier, la conjonction de certains facteurs, tels que la complexité, l'interconnexion, l'interdépendance, l'urgence et la valeur marchande, augmentent le risque de devenir la cible de cybercriminels tels que les « crackers », cybercriminels possédant des « intentions malveillantes ». Ils sont souvent organisés en réseaux mafieux et travaillent pour leur propre compte ou au profit de tiers. Une communauté investie de « bonnes intentions » se dresse face à ces individus, il s'agit des « hackers ». Dans les médias, le terme de hacker est souvent utilisé à tort pour décrire tous les pirates informatiques. Pourtant, ce sont bien souvent les hackers qui signalent les points faibles et attirent l'attention sur leurs conséquences éventuelles ainsi que sur les menaces et les risques potentiels. Ils agissent pour ainsi dire en tant que conscience du marché en matière de sécurité et exhortent les entreprises et les organisations à développer des applications sécurisées ou à remédier aux points faibles identifiés. Les hackers contribuent donc de façon déterminante à la lutte contre les agissements des cybercriminels.

Un tabou brisé

Il y a quelques années seulement, il était encore tabou pour un ministère, une administration, une entreprise ou

une banque d'être associé d'une quelconque manière à cette communauté bigarrée. Mais les choses ont bien changé. Chaque année, les hackers échangent leur savoir d'experts au cours de conférences spécialisées, dédiées à la connaissance et aux développements récents dans les domaines de l'informatique et de la sécurité de l'information. Lors de ces conférences, ils partagent également volontiers leurs connaissances avec d'autres experts, issus de l'industrie, de la lutte contre la criminalité ou de la recherche. Quel que soit leur domaine d'activité (finances, État ou entreprises), les spécialistes informatiques ont ainsi l'occasion de s'informer des failles de sécurité potentielles les plus récentes, des risques et des tendances de la cybercriminalité.

Ces conférences sont extrêmement variées et l'on y trouve de tout : de l'intervenant qui navigue de façon ludique à travers les points faibles de la téléphonie par Internet, en passant par des experts capables de forcer des verrous de sécurité en moins de 30 secondes, jusqu'aux « as des as » qui tentent même de hacker les ordinateurs de crackers. Certains intervenants informent par exemple leur auditoire de la professionnalisation fulgurante de la cybercriminalité. Les visiteurs peuvent y apprendre que les cybercriminels parviennent à obtenir l'accès à des millions d'ordinateurs dans le but d'attaquer des tiers, sans que les utilisateurs privés de ces machines en soient conscients. Le large spectre des sujets traités rend ces conférences d'ailleurs également intéressantes pour les spécialistes d'autres domaines, tels que la pédagogie des médias ou la psychologie.

Il est toujours bon d'écouter

Le professeur Gregory Conti, de la faculté des sciences électroniques et informatiques de l'académie militaire américaine de West Point, résume ses expériences positives, glanées lors de conférences de hackers au cours des quatre dernières années, en ces termes : « Chaque conférence à laquelle nous avons assisté, mes collègues et moi, nous a permis d'acquérir une meilleure compréhension de la diversité de la culture des sciences informatiques ainsi que des vulnérabilités apparaissant dans les mesures de sécurité de nos systèmes. Nous avons de plus en plus d'estime pour l'expertise technique avérée, pour la méthode d'approche lorsqu'il s'agit de trouver une solution à un problème et pour la focalisation que nous y observons. Ces mérites sont pourtant bien souvent marginalisés par les sciences informatiques établies. Or, l'expertise et les solutions des hackers sont supérieures à de nombreux égards à celles de leurs antagonistes dans les laboratoires de recherche ou salles de cours. Les conférences de hackers m'ont permis d'apprendre à respecter les différents horizons et la diversité des disciplines de l'informatique ».

Et c'est un fait : quiconque assiste à des conférences telles que hack.lu, DEFCON, Phreaknic ou encore HOPE ne peut que constater la passion pour l'excellence technique et la volonté d'assimiler de nouvelles connaissances qui animent les intervenants. Ces conférences permettent non seulement d'accroître les connaissances, mais également d'acquérir de nouveaux outils informatiques et de partager des expériences pratiques et des études de cas éthiques.

Le personnel spécialisé et les cadres qui assistent pour la première fois à une telle conférence devraient tenir compte du fait que cela les plongera peut-être dans un environnement nouveau. Mais peu importe l'environnement dont sont issues les personnes qui s'intéressent à la sécurité informatique, elles ont toutes une chose en commun : la passion pour la technique. Toutes souhaitent acquérir une meilleure compréhension des interdépendances techniques et des modes de fonctionnement afin d'écarter les failles de sécurité.

Tous ceux qui souhaitent s'informer sur les points faibles des systèmes embarqués, les possibilités d'attaque sur les réseaux de télécommunications, le crackage de kiosques Internet, la sécurisation de smartcards contre les « sabres lasers » des hackers, les méthodes de classification des malwares, l'authentification de l'utilisateur au niveau des pare-feux, l'analyse de protocoles de réseaux non documentés, les nouveaux concepts de sécurité pour les navigateurs et bien d'autres sujets encore, peuvent assister à la conférence luxembourgeoise de hackers hack.lu, qui se tiendra au mois d'octobre.

Conseil de sécurité :

Conférence luxembourgeoise de hackers d'une durée de trois jours « hack.lu » 2008.

CSRRT-LU (Computer Security Research & Response Team) organise tous les ans, au Luxembourg, la conférence de renommée mondiale hack.lu. Le portail de la sécurité de l'information CASES du Ministère de l'Économie et du Commerce extérieur soutient, avec d'autres sponsors, depuis plusieurs années cet événement dans le domaine de la sécurité de l'information et de la sécurité informatique. Ce sont en particulier les entreprises et organisations luxembourgeoises qui ont ainsi la possibilité de s'informer, pour un prix modique, des récents développements dans ce domaine, d'améliorer les connaissances de leur personnel spécialisé et de mettre en œuvre des mesures de sécurité adéquates. La conférence luxembourgeoise hack.lu 2008 aura lieu sur trois jours, du 22.10. au 24.10.2008, Parc Hotel Alvisse, Ville de Luxembourg. De plus amples informations ainsi qu'un aperçu de tous les exposés prévus sont disponibles sur le site www.hack.lu.

Définition : **hacker**

Les hackers sont des cyberdélinquants qui se contentent de franchir les dispositifs de sécurité plutôt que d'attaquer les systèmes ciblés. Ils souhaitent ainsi mettre en évidence les points faibles de ces systèmes. Le but du hacker est alors plutôt de surmonter un défi technologique. Il ne s'agit pas pour lui de porter préjudice à une entreprise ou organisation, mais plutôt de dévoiler les points faibles des systèmes. Il agit ainsi dans l'intérêt de l'entreprise ou de l'organisation. Une amélioration du système informatique concerné est ainsi possible avant même que des individus malintentionnés soient en mesure d'en exploiter les points faibles. Les hackers sont hautement qualifiés et compétents, peu importe qu'il s'agisse alors de programmeurs chevronnés, de spécialistes réseaux ou de passionnés des technologies de l'information et de la communication.

« Le domaine de l'informatique connaît une interconnexion croissante. L'évaluation des risques devient de plus en plus complexe. Entre-temps, la valeur du marché de la criminalité dans le domaine des systèmes informatiques a dépassé celle du marché de la drogue. Les cybercriminels sont organisés dans des structures professionnelles et possèdent de grandes connaissances spécifiques. Pour cette raison, et également parce qu'ils sont juridiquement responsables et afin d'écarter les préjudices et défaillances éventuels, les cadres et personnels spécialisés devraient acquérir une meilleure connaissance de la sécurité informatique et de la sécurité de l'information, des points faibles éventuels de leurs systèmes, ainsi que des solutions potentielles », conseille François Thill, du portail de la sécurité de l'information CASES.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu