



Plus de 150 hackers au Luxembourg

Pour plus de sécurité, adoptez les réflexes CASES !

Informations importantes pour sécuriser les systèmes informatiques

Ordinateurs portables, ordinateurs de bureau, caractères cryptiques, formules mathématiques, etc. Organisée pour la cinquième fois à Luxembourg du 28 au 30 octobre 2009, la conférence hack.lu de réputation internationale sur la sécurité de l'information permet aux visiteurs de découvrir les points faibles et dangers présents et futurs liés aux technologies numériques.

Le PowerPoint se lit comme un polar. D'un seul petit changement de texte dans un protocole, des systèmes téléphoniques sont mis hors service. De nouvelles formes de logiciels malveillants sont indétectables par les antivirus. Quelques codes de programmation et votre conversation téléphonique est sur écoute.

Même si les experts informatiques ne comprennent pas eux-mêmes toutes les nuances des explications de la conférence, les recommandations découlant des découvertes des hackers, experts en



sécurité et chercheurs sont importantes.

Le point faible du téléphone

Radu State, expert en sécurité à l'Université du Luxembourg, qui met en lumière avec ses collègues Humberto Abdelnur et Jorge Lucangeli Obes, tous deux de l'Institut INRIA de Nancy, les failles des systèmes téléphoniques par le fuzzing, une méthode destinée à trouver les erreurs des logiciels, explique : « Les gens ne pensent pas que les téléphones et systèmes téléphoniques actuels sont plus qu'un simple câble qui

sort d'une prise ». Le mercredi, l'équipe a organisé un atelier pour montrer, d'une part, les faiblesses des systèmes téléphoniques pouvant être exploitées pour planter ou espionner tout le système et, d'autre part, comment automatiser la recherche des failles des systèmes téléphoniques.

Les trois experts ont naturellement mis leur travail à la disposition des entreprises concernées avant toute publication pour que celles-ci aient le temps de corriger les failles constatées. Tous les hackers suivent ce code car ils veulent en fin de compte prendre les criminels de vitesse et aider les utilisateurs finaux, les entreprises, les organisations

et les infrastructures critiques à se protéger des attaques.

Dans un autre atelier dirigé par les experts en sécurité Sandro Gauci et Joffrey Czamy, les participants à la conférence se sont retrouvés le mercredi devant une installation téléphonique actuelle. Un participant a été invité à passer un coup de fil avec l'un des téléphones de l'installation. En plusieurs étapes évocatrices, M. Gauci et M. Czamy ont montré comment les faiblesses de l'installation pouvaient être exploitées de l'extérieur pour que la conversation soit sur écoute sans que l'utilisateur ne s'en aperçoive. Dans la conversation, les deux spécialistes expliquent qu'il convient d'intégrer les réflexions relatives à la sécurité dès le début de la mise en place d'une installation téléphonique dans une organisation ou entreprise. Pour des raisons historiques, ce genre de projet est toutefois encore souvent dirigé par des services en charge de l'organisation des bâtiments de l'entreprise ou organisation alors que les installations reposent sur des technologies numériques nécessitant les connaissances d'informaticiens.

Interrogé sur les méthodes de cryptage contre l'écoute, M. Gauci répond : « Les entreprises et organisations que nous visitons n'ont pas de méthodes de cryptage ».

Conseils de sécurité : conférence hack.lu sur la sécurité de l'information

La conférence sur la sécurité qui se tient le vendredi 30 octobre 2009, à partir de 9h00, au Parc Hotel Alvisse de Luxembourg permet aux organisations et entreprises de s'informer sur les risques possibles et les mesures de sécurité appropriées ainsi que sur les solutions novatrices dans le domaine des technologies numériques. Dans l'édition de cette année, des démonstrations en direct indiquent aux participants la facilité avec laquelle des données confidentielles peuvent être consultées dans des réseaux mal protégés, les réseaux particulièrement susceptibles d'être touchés par des pannes intentionnelles ou non, la manière dont les criminels peuvent infecter des réseaux avec des logiciels malveillants et la façon de les détecter, les outils pouvant aider à créer et à analyser des programmes sûrs ou la manière dont des technologies Internet prisées peuvent entamer des réflexes de sécurité importants et leur exploitation par des criminels.

Sont également au programme de ce vendredi des exposés sur l'exploitation de failles dans le langage de programmation Delphi, des astuces pour contourner le protocole de sécurité SSL, ce qui se passe si E.T. arrive sur Windows Mobile 6 ou les stratégies de défense par le biais de données incorrectes fournies au système d'exploitation. Parallèlement à cela, les participants peuvent s'exercer au crochetage de verrous ou, de façon très pratique, au soudage de platines.

Les exposés démontreront aux entreprises et organisations qu'une politique de sécurité bien organisée est nécessaire et doit être confiée à des experts correctement formés. Il convient de souligner à ce propos qu'un master « Management de la sécurité des systèmes d'information » (MSSI) est proposé à l'Université du Luxembourg, fruit de la collaboration entre cette dernière, le Centre de recherche CRP Henri Tudor et Clussil (association des spécialistes de la sécurité informatique au Luxembourg). Ce cursus propose un mélange interdisciplinaire de technique, d'économie et de droit, qui se reflète aujourd'hui dans la pratique de la sécurité de l'information. Il s'intéresse aux risques, aux normes et aux directives qui aident les entreprises à rendre leur sécurité interne mesurable, contrôlable et optimisable. Le prochain cursus démarrera au printemps 2010. Pour de plus amples informations : <http://tools.cases.lu/925>.

L'absence d'une telle mesure de protection laisse penser

que les décideurs n'ont pas les connaissances nécessaires sur les failles, dangers et répercussions possibles. Certes, il est complexe de pénétrer dans un tel réseau de l'extérieur pour écouter des informations, mais les entreprises devraient toujours tenir compte du maillon faible que sont les collaborateurs, surtout lorsqu'il n'y a pas eu de sensibilisation au thème de la sécurité de l'information. On connaît par exemple des cas en France où des pirates avaient gagné beaucoup d'argent par le vol de numéros de téléphone en mettant sur la facture d'un client final des appels à l'étranger qu'il n'avait jamais passé mais devait payer parce qu'il ne pouvait pas prouver que des tiers étaient à l'origine de ces appels. M. Czamy ajoute : « La technologie Voice over IP, c'est-à-dire les appels passant par des protocoles Internet, présente les mêmes points faibles et est confrontée aux mêmes menaces qu'un serveur d'e-mails. » Même dans le domaine de la téléphonie, les entreprises de taille moyenne ont désormais besoin de connaissances informatiques appropriées.

Un exposé présenté le même jour aborde les points faibles de l'iPhone, un appareil très prisé. L'expert en sécurité responsable de la présentation parle des lacunes lorsque l'appareil utilise des connexions

Internet sans fil comme le WiFi. Le flux de données du téléphone mobile peut être surveillé par des applications liées à Facebook. Un accès de tiers à l'application utilisée est ainsi possible. L'intervenant estime que cette faille est plus que vraisemblablement présente aussi sur d'autres applications iPhone.

Ce qu'il faut savoir sur les technologies numériques

Un autre exposé intéressant a également été présenté sur les problèmes de sécurité représentés par les modules de Mozilla Firefox qui ne devraient être téléchargés qu'à partir de sites dignes de confiance car ils possèdent les mêmes droits d'accès sur l'ordinateur qu'un utilisateur, c'est-à-dire en général les droits d'administrateur. Les modules falsifiés ou manipulés par des pirates peuvent donc constituer une faille à haut risque. La sensibilisation des utilisateurs et l'adoption de réflexes de sécurité sont particulièrement nécessaires ici.

Beaucoup d'informaticiens peuvent se réjouir à la perspective de l'analyse du fichier journal, comme l'explique l'expert en sécurité Jan P. Monsch. Le logiciel Open Source GGobi permet la représentation visuelle d'anomalies sur le trafic du réseau. Il fait gagner beaucoup de temps aux responsables de la sécurité

de l'information en surveillant le réseau pour le protéger contre les attaques.

En revanche, un exposé sur les formes possibles de logiciels malveillants peut donner la migraine. Anthony Desnos montre ainsi dans son exposé que des virus peuvent se diviser pour ne pas être repérés par des antivirus.

Le Chaos Computer Club de Luxembourg présente une conférence sur les empreintes digitales. Un film et un adhésif rapide suffisent à les reproduire. Les hackers présents du club expliquent que, comme mesure de sécurité, beaucoup d'ordinateurs portables sont aujourd'hui équipés d'un dispositif d'identification des empreintes digitales. Il a été prouvé que plus de trois quarts de ces systèmes de reconnaissance peuvent être contournés par une empreinte digitale copiée, par exemple à partir d'un bonbon en gélatine. Un hacker luxembourgeois déclare à ce propos : « Ce n'est pas compliqué d'obtenir une empreinte digitale car tout ordinateur portable est justement couvert d'empreintes de son utilisateur ».

Le Hackerspace de Luxembourg qui met à la disposition des hackers et des mordus d'informatique de la région une infrastructure et une plateforme d'échange démontre au public intéressé

comment l'art et les technologies informatiques peuvent être conciliés, par exemple via Arduino, un microcontrôleur. On utilise ici des LED lumineuses, de la programmation et de la microélectronique.

Les hackers et experts en sécurité de 15 pays se sont donné pour mission de découvrir les failles de sécurité de programmes et réseaux par un esprit de découverte et des méthodes non conventionnelles. Ils ne

considèrent toutefois leur tâche remplie que lorsqu'ils ont trouvé des propositions de solution créatives. Passés maîtres dans leur pratique, ils empruntent des voies novatrices et inhabituelles. Comme les hackers viennent d'horizons professionnels très divers, ils abordent le sujet de la sécurité de l'information sous des angles aussi variés que l'économie, la politique, la société et le droit. Leurs découvertes et conclusions servent à enrichir la recherche et le

développement de technologies et réseaux sûrs. Le climat général de bricolage en inspirera certainement quelques-uns pour envisager la sécurité de l'information sous un jour nouveau. Même les non-professionnels tireront profit de la meilleure exploitation des outils courants et de leur utilisation alternative.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu