WOW!

Un mot de passe sécurisé doit comprendre au moins huit caractères et contenir des lettres (minuscules et majuscules), des chiffres ainsi que des signes spéciaux.

En 2014, la cybercriminalité a provoqué un préjudice économique d'environ 200 millions de francs.

Le plus grand vol de données de tous les temps: à l'été 2014, des hackers russes ont volé 4,5 milliards de combinaisons nom d'utilisateur–mot de passe dans le monde entier.

Oracle Java, Adobe Reader ou Adobe Flash sont installés sur 99 pour cent de tous les ordinateurs. Toutes ces machines sont donc vulnérables aux cyberattaques.

Les réseaux sociaux sont également un terrain de jeu apprécié des cybercriminels: les faux sites de fans, les programmes malveillants qui se propagent en quelques clics, ou encore les faux messages ciblés, sont autant de pièges dans lesquels peuvent tomber les utilisateurs de réseaux sociaux.

La société de sécurité américaine Norse a visualisé la lutte virtuelle sur Internet dans une carte interactive. Celle-ci démontre qu'à chaque seconde, des attaques peuvent être menées contre des installations de sociétés dans le monde entier. http://map.norsecorp.com

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Le magazine de la technique pour les jeunes

TechnoScope by SATW 3/15

Cybersécurité

Internet est loin d'être un monde idéal. Qu'est-ce que cela signifie pour nos smartphones et autres appareils portables?

Avec concours

En quoi consiste le tracking?

Ne t'es-tu jamais demandé pourquoi, lorsque tu fais une recherche sur Google ou sur d'autres sites Web, des publicités apparaissent concernant des choses que tu as recherchées récemment? Comment Internet peut-il savoir tout à coup que je recherche une nouvelle chaîne stéréo ou des vacances en Italie? La réponse est simple: chaque ordinateur et chaque smartphone est identifiable de manière univoque via son adresse IP. Lors d'une recherche, l'«adresse» est toujours envoyée au serveur qui répond à notre demande. Grâce au protocole HTTP, les exploitants des sites Web savent d'où provient la demande et de quel type d'appareil.

De plus, les serveurs Web collectent à tout moment des données concernant nos préférences personnelles. Généralement, cela se déroule discrètement. Ce «sondage» réalisé à des fins publicitaires ou de surveillance est appelé «tracking». De petits fragments de texte – appelés «cookies»– sont stockés dans le navigateur (par exemple Firefox, Safari ou Internet Explorer). Grâce à ces cookies, les exploitants des sites Web peuvent collecter des données qui leur permettent de déduire l'âge, le sexe, l'emplacement, le domicile, l'employeur et la nationalité de l'utilisateur. De plus, lorsque l'utilisateur divulgue lui-même des données personnelles, par exemple lorsqu'il participe à un concours, celles-ci peuvent être attribuées non seulement à un ordinateur, mais également à une personne. Les exploitants des sites Web vendent ensuite ces données à des groupes publicitaires qui souhaitent adapter leurs publicités aux différents surfeurs sur Internet.

Cookies: Les sites Web professionnels mémorisent ce que recherchent les surfeurs sur Internet, par exemple un livre spécifique. Ces informations sont enregistrées dans le navigateur au moyen de petits paquets d'informations appelés «cookies». Lorsque je retourne sur le même site, le serveur Web du fournisseur récupère des informations sur le livre qui m'intéressait au moyen des cookies du navigateur. C'est pourquoi il apparaît subitement dans la fenêtre publicitaire. Les cookies peuvent être bloqués ou supprimés dans les paramètres du navigateur.

Apps: De nombreuses applications sont particulièrement insidieuses en termes d'enregistrement dissimulé des données. Elles possèdent leurs propres canaux de communication et déterminent elles-mêmes quelles données sont collectées et transmises sur mon smartphone. En acceptant les conditions générales (CG) du fabricant, j'exprime mon consentement. Comme les smartphones sont des appareils très personnels, les fournisseurs d'applications peuvent accéder à des données très personnelles, par exemple les noms d'utilisateurs, les adresses, les numéros de téléphone, les contacts, le calendrier, l'âge, le sexe et la localisation (via géolocalisation et GPS). «Whatsapp», l'une des applications les plus populaires au monde, a fait l'objet de critiques répétées de la part des responsables de la protection des données. La société a en effet accès libre à toutes les communications se déroulant via l'application.

Likes sur Facebook: Toute personne sur Internet qui «like» des commentaires ou des produits indique à Facebook ce qui lui plaît. Par exemple des super sneakers ou certaines positions politiques. Facebook combine ces informations avec les données du profil Facebook, puis en déduit les produits et les offres susceptibles d'intéresser l'utilisateur. Facebook vend ensuite ces informations à des annonceurs qui publient sur Internet la publicité qui incitera l'utilisateur à acheter.

Prof. Solange Ghernaouti,
Swiss Cybersecurity Advisory and
Research Group, université de Lausanne

«Plus nous divulguons des données personnelles, plus nous sommes vulnérables»

Aujourd'hui, chacun doit se protéger contre les attaques sur Internet, telle est la conviction de Solange Ghernaouti. Cette professeure en cybercriminalité à l'université de Lausanne explique dans cette interview pourquoi les cybercriminels ne sont presque jamais arrêtés et pourquoi nous faisons leur jeu avec les médias sociaux.

Madame Ghernaouti, existe-t-il aujourd'hui des exemples d'attaques cybercriminelles de grande envergure?
Aux États-Unis, il y a eu effectivement un cas où l'alimentation électrique d'une ville a été piratée et paralysée. La cybercriminalité représente déjà un grand danger pour les Etats et les entreprises et devrait être traitée comme un thème central de la politique de sécurité nationale. Cet été, les données personnelles de 37 millions d'utilisateurs du service Internet «Ashley Madison» ont été volées par des inconnus. Il s'agit d'un service de rencontre en ligne dont les utilisateurs supposaient que leurs données étaient conservées en toute sécurité et qu'ils naviguaient de façon anonyme sur cette plateforme. Mais cela s'est avéré un leurre. Pour de nombreuses personnes, les effets sur leur vie privée et professionnelle ont été désastreux.

Sommes-nous tous potentiellement vulnérables face à la cybercriminalité?
Evidemment! Sur Internet, on constate régulièrement des cas de fraude. Grâce à Internet, il est devenu très simple pour les criminels de faire chanter des victimes et de les mettre sous pression. Aujourd'hui, chacun est exposé à des risques et la plupart des utilisateurs Internet sont incapables de se défendre, car ils ne disposent pas des technologies et des connaissances nécessaires. Il ne suffit plus aujourd'hui d'installer un logiciel antivirus.

Mais quelqu'un qui agit avec prudence sur Internet et n'est pas dupe des escroqueries par e-mail peut surfer en toute sécurité, non?
Pas forcément. Aujourd'hui, beaucoup de choses se déroulent de façon cachée. Des données personnelles peuvent être volées sans que l'on remarque quoi que ce soit. Ce n'est pas la même chose lorsque je perds mon portemonnaie et que je sais précisément quelle carte je dois bloquer.

Que peut-on faire pour mieux se protéger contre ces attaques et ces vols?
Pour ne pas courir de risques inutiles, il faut divulguer le moins de données possible sur Internet. Plus une personne fournit des données sur Internet, plus il est simple pour les criminels de l'escroquer, de lui extorquer de l'argent ou de manipuler son identité sur le Web. Grâce à la multitude de données disponibles sur Internet, les cybercriminels nous connaissent généralement beaucoup mieux que nous nous connaissons nous-mêmes. Plus nous utilisons des services Internet et des médias sociaux, plus nous sommes vulnérables. C'est très dangereux!

Comment éviter ces risques?
J'utilise Internet uniquement à des fins professionnelles. Je ne communique pas via les médias sociaux et je n'achète pas non plus sur Internet. J'essaie donc de réduire autant que possible les données me concernant.

A quel point les médias sociaux sont-ils critiques en termes de cybercriminalité?
Facebook, Twitter, Linkedin et d'autres services sont le point de mire des cybercriminels, car les personnes y divulguent une très grande quantité de données personnelles. La plupart des médias sociaux ne sont pas en mesure de garantir la sécurité des données personnelles.

«La plupart des médias sociaux ne sont pas en mesure de garantir la sécurité des données personnelles.»

Comment peut-on améliorer la sécurité du cyberespace?
Nous devons avant tout inciter les grandes sociétés Internet à lutter contre la vulnérabilité de leurs utilisateurs et les failles de sécurité du système. Même s'ils apprennent à évoluer avec prudence sur Internet, les utilisateurs Internet n'ont aucun contrôle sur les failles de sécurité du système.

A quel point est-ce difficile pour la police de lutter contre les cybercriminels?
Aujourd'hui encore, la police est quasi impuissante. La cybercriminalité ne s'arrête pas aux frontières et les traces dans le cyberespace sont très faciles à effacer. Il est donc extrêmement difficile d'identifier les auteurs d'une attaque. Les criminels peuvent se trouver n'importe où dans le monde et s'introduire dans mon ordinateur. De plus, il arrive souvent que les particuliers aient trop honte pour contacter la police. Les cybercriminels le savent et en profitent sans aucun scrupule.

La Suisse est-elle bien préparée pour faire face aux cyberattaques?
Pas vraiment. On prend de plus en plus conscience de l'urgence du problème, mais les ressources et les mesures concrètes font encore défaut. Jusqu'à présent, seules deux affaires ont été portées devant le Tribunal fédéral, même si nous savons que les délits sont beaucoup plus nombreux.

Avez-vous vous-même été victime de cybercriminels?
Oui, au début de l'année 2015, après les attentats contre la rédaction de l'hebdomadaire satirique «Charlie Hebdo» à Paris, de nombreux sites Web francophones consacrés à la cybersécurité ont été attaqués. Mon site Web a également été paralysé. Cela m'a fait peur, c'était une sorte de terrorisme. Il m'a fallu deux jours de travail pour relancer le site Web.

Les infrastructures critiques – les usines électriques et hydrauliques, les sociétés de télécommunication ou de transport, mais aussi les banques et les grands hôpitaux - sont de plus en plus la cible des hackers.

Des attaques critiques en provenance d'Internet

Ces dernières années, les attaques criminelles sur Internet ont sensiblement augmenté. Du fait de la connectivité croissante, les infrastructures critiques sont de plus en plus touchées. Toutes ne sont pas bien protégées contre de telles attaques.

Fin novembre 2014, deux groupes inconnus ont entièrement paralysé le réseau de la société Sony Pictures Entertainment pendant plusieurs jours. Les pirates ont déclaré être en possession d'informations secrètes de l'entreprise et ont menacé de les publier. Et en effet, quelques jours plus tard, cinq films inédits ont fait leur apparition sur les plateformes d'échange Internet. Le FBI a conclu par après que cette attaque avait été menée par le gouvernement nord-coréen qui voulait empêcher la sortie du film «The Interview». Cette comédie relate un complot d'assassinat contre le dirigeant nord-coréen Kim Jong-un.

Des cyberattaques aussi spectaculaires suscitent une grande attention dans les médias. Mais elles tendent à être l'exception, du moins d'après ce que sait le public. Les petites attaques furtives sont beaucoup plus fréquentes. Les hackers tentent de trouver les failles du dispositif de défense le plus discrètement possible afin d'accéder par exemple à des informations sensibles ou de voler de l'argent sur les comptes bancaires. Ces attaques sont perfides car les personnes concernées ne se rendent compte souvent que trop tard qu'elles ont été attaquées. Et lorsqu'elles le remarquent, il n'est pas toujours facile pour elles de savoir qui se cache derrière ces attaques.

Des menaces pour la société

Ces dernières années, les attaques menées contre les installations industrielles ont également augmenté. L'une des plus célèbres attaques est celle du ver informatique Stuxnet qui aurait été utilisé par les Américains ou les Israéliens pour attaquer délibérément une usine d'enrichissement d'uranium en Iran en 2010. L'année dernière, l'Allemagne a également connu un cas spectaculaire: dans une aciérie, des hackers inconnus sont parvenus à manipuler le logiciel de contrôle d'un haut fourneau afin d'endommager l'infrastructure.

Les attaques ciblées contre les installations techniques pourraient également toucher la Suisse. Pour protéger au mieux notre pays contre ces attaques, la Confédération a créé le service «Melani». D'une part, les experts de la Confédération mettent à disposition des informations accessibles au public, qui permettent aux sociétés ainsi qu'aux particuliers de mieux se protéger. D'autre part, Melani travaille en étroite collaboration avec les exploitants d'infrastructures critiques. Il s'agit d'institutions dont le fonctionnement est indispensable à la société, p. ex. les usines électriques et hydrauliques, les sociétés de télécommunication ou les entreprises de transport, mais également les banques et les grands hôpitaux.

Les secteurs sont différemment équipés contre ces attaques, explique Pascal Lamia, responsable du service. Alors que les banques ont très bien protégé leur infrastructure IT, les entreprises d'électricité se trouvent dans une situation difficile: le secteur de l'électricité subit en effet une restructuration qui engendre de nouveaux risques. De nouvelles technologies électriques sont constamment raccordées au réseau; dans le même temps, les sociétés doivent réaliser des économies.

Des hôpitaux difficiles à maîtriser

Selon Lamia, la situation est critique avant tout dans les hôpitaux où la connectivité a connu une expansion rapide ces dernières années. Par exemple, il est impossible désormais d'effectuer une opération sans avoir une infrastructure IT performante. «Le problème est lié au fait que les hôpitaux utilisent de nombreux appareils interconnectés dont le fonctionnement et le niveau de protection sont différents. Etant donné la forte pression des coûts, cela représente un grand défi pour chaque hôpital.»

Lamia estime toutefois qu'un autre secteur court un plus grand risque: les petites et moyennes entreprises. Pour des raisons personnelles et financières, contrairement aux grandes entreprises, celles-ci ne sont généralement pas en mesure de se protéger suffisamment contre les cyberattaques. Les petites entreprises sont de plus en plus souvent la cible du chantage des cybercriminels. Les hackers menacent par exemple des sociétés, qui vendent des produits sur Internet, de paralyser leur site Web si elles ne leur versent pas un certain montant. Bien que la Confédération déconseille vivement de répondre à ces demandes, Lamia sait que certaines sociétés ont payé la somme réclamée, car la défaillance de leur site aurait occasionné des coûts encore plus élevés.

Le smartphone: un facteur de risque

Le smartphone occupe une place de plus en plus grande dans notre vie. Chaque jour, nous envoyons d'innombrables messages via cet appareil mobile et enregistrons une grande quantité de données personnelles sur cet appareil pratique – par exemple des photos ou des données d'applications de santé. C'est précisément pour cette raison qu'il est essentiel que chaque utilisateur s'inquiète de la sécurité des données. Que se passe-t-il par exemple en cas de perte ou de vol de l'appareil? Les données sont-elles irrémédiablement perdues? Et que se passe-t-il si ces informations tombent dans de mauvaises mains?



Nicholas Hansen a participé pour la troisième fois au concours Cyber Security Challenge. Lors de la finale suisse, les équipes ont dû prouver leurs capacités de multiples façons.

▸ Nicholas Hansen: «Pour avoir du succès en tant que hacker, il faut avoir du flair pour trouver le point faible d'un système, et aussi faire preuve de patience.»

Un jeu sérieux

Comment se protéger contre les attaques Internet? Cette question fascine Nicholas Hansen. Cet automne, ce jeune homme de 19 ans a démontré lors du Cyber Security Challenge qu'il était l'un des meilleurs hackers de Suisse dans sa catégorie d'âge.

En fait, c'est par hasard que j'ai découvert mon sujet de prédilection: la cybersécurité. Durant ma deuxième année d'apprentissage en informatique, nous avions à l'école un module dédié à la sécurité sur Internet, et ce domaine m'a tout de suite fasciné. J'y ai même consacré une partie de mon temps libre. Un jour, un collègue m'a parlé du «Cyber Security Challenge». Il pensait que c'était fait pour moi. Et il avait raison.

Cette année, j'ai participé pour la troisième fois au concours pour la relève organisé par l'association Swiss Cyber Storm. En raison du grand nombre de participants, cette année, les sélections se sont déroulées autrement que les années précédentes: lors de la phase de qualification, chaque participant a dû résoudre seul des tâches spécifiques. Ceux d'entre nous qui ont réussi cette phase ont pu participer à la finale suisse qui s'est déroulée à Sursee à la mi-septembre. Répartis en petites équipes, nous devions résoudre des tâches complexes, par exemple trouver des failles de sécurité dissimulées dans des applications Web, craquer des documents cryptés ou nous créer un accès à un système protégé.

Pour les 10 meilleurs d'entre nous, l'aventure s'est poursuivie: en octobre, nous avons participé à la finale européenne qui s'est déroulée en Suisse au KKL de Lucerne. Nous avons dû y affronter des équipes venues d'Allemagne, d'Autriche, d'Angleterre, d'Espagne et de Roumanie. Chaque équipe se composait de dix membres et disposait de son propre serveur Web sur lequel s'exécutaient des applications comportant certaines lacunes. Notre tâche consistait à sécuriser ces applications et corriger les points faibles. Parallèlement, nous devions essayer de pénétrer dans les serveurs des équipes concurrentes.

Notre équipe s'est préparée de façon intensive à cette finale. Nous avons créé un dépôt centralisé dans lequel nous avons consigné tous nos outils, ainsi qu'un canal de chat commun. Nous avons clairement défini qui était responsable de quoi dans notre équipe. J'étais pour ma part chargé de détecter au plus vite les attaques des autres équipes. Il était intéressant de voir comment les autres nous attaquaient, car cela nous donnait des indications sur la manière dont nous pouvions craquer leurs systèmes. Malheureusement, cela n'a pas suffi pour gagner. Nous avons terminé à la troisième place.

Pour le moment, je me consacre à la cybersécurité surtout pendant mon temps libre. Pour moi, tout cela est une sorte de jeu: j'aime beaucoup résoudre des problèmes, attaquer les autres et me défendre contre leurs attaques. Après avoir résolu une tâche difficile, cela me donne un sentiment de satisfaction. Lorsque mes idées sont infructueuses, c'est parfois frustrant, mais cela me pousse également à aller de l'avant. Pour avoir du succès en tant que hacker, il faut avoir du flair pour trouver le point faible d'un système. Par exemple, lorsque je vois un formulaire d'entrée sur un ancien site Web, j'ai tout de suite envie de savoir si l'infrastructure derrière ce formulaire présente un point faible. Ou quand un mot de passe a été enregistré sous une forme cryptée dans un programme, je veux découvrir où cela a été fait et selon quel modèle le chiffrement a été réalisé.

Pour avoir du succès en tant que hacker, il faut aussi faire preuve de patience et tenter sans cesse de nouvelles choses. Généralement, le temps passe trop vite, et il arrive souvent que je reste planté devant mon ordinateur jusque tard dans la nuit. Parfois, il me faut plusieurs jours pour résoudre une tâche. Il n'est pas simple alors pour moi de déconnecter. J'y parviens plus facilement lorsque je m'arrête immédiatement parce que j'ai trouvé une bonne idée. Je ne suis pas tenté alors de continuer encore et encore.

Pour le moment, je travaille toujours dans mon entreprise d'apprentissage. En tant qu'informaticien, je suis responsable du fonctionnement de l'infrastructure IT interne. Après l'école de recrues, je ferai certainement des études en informatique. Je m'imagine très bien travailler plus tard dans le domaine de la sécurité, car c'est un domaine très important pour la société. Aujourd'hui, de plus en plus d'appareils, qui doivent fonctionner de manière fiable, sont interconnectés. Cela augmente bien entendu le risque qu'ils soient paralysés par des attaques Internet. Lorsque l'on sait où se trouvent les points faibles, il est possible de mieux protéger l'installation.

AHA!

AHA: En quoi consiste le chiffrement?

Lors du chiffrement, un texte clair, autrement dit un texte lisible normalement, est converti en un «texte crypté» qui semble dénué de sens. Dans l'ancienne Egypte, des messages importants étaient déjà retranscrits en textes cryptés pour empêcher qu'ils ne soient lus s'ils venaient à tomber dans de mauvaises mains lors de la transmission. Aujourd'hui, le chiffrement sert avant tout à sécuriser la transmission des informations par les canaux numériques tels qu'Internet. Le chiffrement des e-mails permet par exemple à un expéditeur d'envoyer des messages confidentiels à un destinataire sans qu'ils ne puissent être lus par une tierce personne. Il est nécessaire pour cela d'utiliser une «clé». Dans les procédés de chiffrement informatiques modernes, il s'agit d'une séquence binaire, autrement dit d'un nombre très long composé de zéros et de uns. A l'heure actuelle, les procédés de chiffrement usuels se basent une sécurité relative. La charge de calcul pour craquer une clé doit être suffisamment grande pour que celle-ci ne puisse être craquée dans un délai raisonnable avec un matériel informatique usuel.

Symétrique ou asymétrique

En principe, on distingue deux types de chiffrement. Les procédés de chiffrement symétriques utilisent la même clé secrète pour le chiffrement et le déchiffrement. En revanche, dans le chiffrement asymétrique, la clé utilisée pour chiffrer le texte clair est différente de celle utilisée pour déchiffrer le texte crypté. La clé de chiffrement est publique, autrement dit connue des autres utilisateurs. En revanche, la clé de déchiffrement est secrète.

La cryptologie est la science qui s'occupe de la sécurité des informations. Elle inclut les disciplines de la cryptographie, qui traite du chiffrement, et de l'analyse cryptique qui s'intéresse au craquage du chiffrement.

www.satw.ch/concours

Formation

Quiconque souhaite devenir expert en cybersécurité a besoin de bonnes connaissances en informatique. En Suisse, les formations en informatique sont proposées par le biais d'apprentissages ainsi que dans les hautes écoles spécialisées et dans la plupart des universités, y compris l'ETH Zurich et l'EPFL.

Un aperçu des possibilités de formation est disponible sur
www.berufsberatung.ch > Choix professionnel > Toutes les professions > Informatique > Recherche

Les débouchés professionnels dans le domaine de la sécurité – également concernant les aspects de sécurité dans le monde réel – sont très nombreux:
www.berufsberatung.ch > Choix professionnel > Toutes les professions > Sécurité > Recherche

Concours

Que sais-tu de la cybersécurité? Teste tes connaissances, participe au concours et gagne l'un des trois bons de Digitec d'une valeur de 150 francs. Un bon te permet par exemple d'acheter un programme de sécurité qui protégera ton ordinateur contre les cyberattaques, et de faire bien d'autres choses. Le concours est ouvert jusqu'au 30 avril 2016.
www.satw.ch/concours

Impressum

SATW Technoscope 3/15, décembre 2015
www.satw.ch/technoscope

Concept et rédaction: Beatrice Huber
Collaboration rédactionnelle: Felix Würsten, Samuel Schläfli
Photos: Fotolia, Swiss Cyber Storm, Nicholas Hansen, Solange Ghernaouti

Abonnement gratuit et commandes supplémentaires
SATW, Gerbergasse 5, CH-8001 Zurich
technoscope@satw.ch, Tél: +41 (0)44 226 50 11

Le Technoscope 1/16 paraîtra en mai 2016 et aura pour thème «Tunnel de base du Gothard».