WOW!

Ein sicheres Passwort sollte mindestens acht Zeichen lang sein und sowohl Buchstaben (kleine und grosse), Zahlen als auch Sonderzeichen enthalten.

Cyberkriminalität verursachte in der Schweiz 2014 einen volkswirtschaftlichen Schaden von rund 200 Millionen Franken.

Der grösste Datendiebstahl aller Zeiten: Russische Hacker haben im Sommer 2014 rund um die Welt 4,5 Milliarden Benutzernamen-Passwort-Kombinationen gestohlen.

Oracle Java, Adobe Reader oder Adobe Flash sind auf 99 Prozent aller Computer installiert. Alle diese Maschinen sind deshalb anfällig für Cyber-Attacken.

Auch soziale Netzwerke sind ein beliebtes Tummelfeld von Cyberkriminellen: Gefälschte Fan-Seiten, Schadprogramme, die sich durch Klicks verbreiten, oder gezielte Falschmeldungen sind Fallen, in welche die Nutzer von sozialen Netzwerken tappen können.

Den virtuellen Kampf im Internet hat der amerikanische Sicherheitsanbieter Norse in einer interaktiven Karte visualisiert. Sie zeigt, wie im Sekundentakt Angriffe aus aller Welt auf verschiedenste Einrichtungen unternommen werden. 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

Das Technikmagazin für Junge und Junggebliebene

TechnoScope by SATW 3/15

Cyber Security

Auch im Internet herrscht keine heile Welt. Was heisst das nun im Umgang mit unserem Smartphone und co?

Mit Wettbewerb

Wie funktioniert Tracking?

Hast du dich schon Mal gefragt, weshalb bei der Google-Suche oder auf anderen Webseiten gerade diejenigen Dinge beworben werden, nach welchen du kürzlich gesucht hast? Wieso weiss das Internet plötzlich, dass ich eine neue Stereoanlage oder in die Ferien nach Italien will? Die Antwort ist einfach: Über die IP-Adresse ist jeder Computer und jedes Smartphone eindeutig identifizierbar. Bei einer Suchanfrage wird die eigene «Adresse» stets an denjenigen Server mitgeschickt, von dem aus unsere Anfrage beantwortet wird. Über das HTTP-Protokoll wissen die Betreiber von Webseiten, woher und von was für einem Gerät die Anfrage kommt.

Darüber hinaus sammeln Webserver jederzeit Daten zu unseren persönlichen Vorlieben. Meist läuft dies im Verborgenen ab. Dieses «Aushorchen» für Werbezwecke oder zur Überwachung nennt man Tracking. Dabei werden im Browser (zum Beispiel Firefox, Safari oder Internet Explorer) kleine Textschnipsel – Cookies genannt – hinterlegt. Über diese können Betreiber von Webseiten Daten sammeln, die Rückschlüsse zu Alter, Geschlecht, Aufenthaltsort, Wohnort, Arbeitgeber und Nationalität des Nutzers ermöglichen. Wenn der Nutzer zudem persönliche Daten von sich preisgibt, zum Beispiel bei der Anmeldung für ein Quiz, können diese nicht nur einem Computer, sondern auch einer Person zugeordnet werden. Diese Daten verkaufen die Betreiber von Webseiten später an Werbekonzerne, die daran interessiert sind, ihre Werbung perfekt auf den einzelnen Internet-Surfer anzupassen.

Cookies: Professionelle Webseiten merken sich, nach was Surfer im Internet suchen, zum Beispiel nach einem bestimmten Buch. Diese Informationen werden über kleine Informationspakete, so genannte Cookies, im Browser abgespeichert. Beim erneuten Surfen auf dieser Website holt sich der Webserver des Anbieters über die Cookies im Browser Informationen darüber, für welches Buch ich mich zuvor interessiert hatte. Deshalb erscheint dieses nun plötzlich im Werbefenster. Cookies lassen sich in den Browser-Einstellungen sperren oder löschen.

Apps: Viele Apps sind punkto verborgener Datenaufzeichnung besonders heimtückisch. Sie haben eigene Kommunikationskanäle und bestimmen selbst, welche Daten auf meinem Smartphone gesammelt und übermittelt werden. Indem ich die Allgemeinen Geschäftsbedingungen (AGB) des Herstellers annehme, gebe ich mein Einverständnis dazu. Da Smartphones sehr persönliche Geräte sind, können App-Anbieter darüber Zugriff auf sehr persönliche Daten kriegen. Zum Beispiel auf Nutzernamen, Adressen, Telefonnummern, Kontakte, Kalender, Alter, Geschlecht und den eigenen Standort (über Geolokalisation und GPS). «Whatsapp», eine der weltweit beliebtesten Apps, wurde von Datenschützern immer wieder kritisiert. Die Firma hat unter anderem freie Einsicht in sämtliche über die App laufende Kommunikation.

Facebook-Likes: Wer im Internet Kommentare oder Produkte «liked», der teilt Facebook mit, was er gerne mag. Zum Beispiel coole Sneakers oder bestimmte politische Haltungen. Facebook kombiniert diese Information mit den Daten aus dem eigenen Facebook-Profil und leitet daraus ab, welche Produkte und Angebote den Nutzer interessieren könnten. Dieses Wissen verkauft Facebook an Werbetreibende, die dafür sorgen, dass der Internet-Nutzer möglichst diejenige Werbung im Internet sieht, die ihn zu einem bestimmten Kauf anregt.

«Man sollte möglichst wenig Daten von sich im Internet preisgeben.»

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

«Je mehr Daten wir von uns preisgeben, desto angreifbarer werden wir»

Jeder und jede muss sich heute gegen Übergriffe im Internet schützen, davon ist Solange Ghernaouti überzeugt. Die Professorin für Cyberkriminalität an der Universität Lausanne erklärt im Interview, weshalb Cyberkriminelle fast nie gefasst werden und weshalb wir ihnen mit den sozialen Medien in die Hände spielen.

Frau Ghernaouti, gibt es heute schon Beispiele für grossangelegte cyberkriminelle Attacken?
In den USA gab es einen Fall, wo die Stromversorgung einer Stadt gehackt und lahmgelegt wurde. Cyberkriminalität ist für Staaten und Unternehmen heute bereits eine grosse Gefahr und sollte als Schlüsselthema der nationalen Sicherheitspolitik behandelt werden. Diesen Sommer wurden zudem die persönlichen Daten von 37 Millionen Nutzer des Internetdienstes «Ashley Madison» von Unbekannten gestohlen. Das ist ein Online-Dating-Service und die Nutzer gingen davon aus, dass ihre Daten sicher aufgehoben sind und sie sich auf dieser Plattform anonym bewegen. Das hat sich als Trugschluss herausgestellt. Für viele Menschen hatte dies schwerwiegende Folgen für ihr Privat- und Berufsleben.

Sind wir also alle potentiell durch Cyberkriminalität gefährdet?
Auf jeden Fall! Im Internet kommt es immer wieder zu Betrugsfällen. Durch das Internet wurde es für Kriminelle sehr einfach Opfer zu erpressen und sie unter Druck zu setzen. Jeder ist heute einem Risiko ausgesetzt und die meisten Internet-Nutzer können sich nicht dagegen wehren, weil sie die Technologien und das Wissen dazu nicht haben. Einfach nur eine Antivirus-Software zu installieren genügt heute nicht mehr.

Aber wer im Internet etwas vorsichtig ist und nicht auf Betrügereien per E-Mail hineinfällt, der kann trotzdem sicher surfen, oder?
Nicht unbedingt. Vieles läuft heute im Verdeckten ab. Persönliche Daten können gestohlen werden, ohne dass ich das Geringste davon bemerke. Das ist anders, als wenn ich mein Portemonnaie verliere und dann genau weiss, welche Karten ich sperren muss.

Was kann jeder einzelne tun, um sich besser vor solchen Angriffen und Diebstählen zu schützen?
Um sich nicht unnötig Risiken auszusetzen, sollte man möglichst wenig Daten von sich im Internet preisgeben. Denn je mehr Daten zu einer Person im Internet verfügbar sind, desto einfacher ist es für Kriminelle diese zu betrügen, für Geld zu erpressen oder deren Identität auf dem Web zu manipulieren. Die Cyberkriminellen wissen durch die Vielfalt an Daten im Internet oft besser über uns Bescheid, als wir selbst. Je mehr wir also Internet-Dienste und Social Media nutzen, desto verwundbarer machen wir uns. Das ist sehr gefährlich!

Wie gehen Sie selbst mit diesem Risiko um?
Ich benutze das Internet nur für berufliche Zwecke. Ich kommuniziere nicht über Social Media und kaufe auch nicht über Internet ein. So versuche ich die über mich verfügbaren Daten möglichst gering zu halten.

Wie kritisch sind Social Media punkto Cyberkriminalität?
Facebook, Twitter, Linkedin und andere Dienste stehen im Fokus der Cyberkriminellen, weil Menschen dort sehr viel persönliche Daten von sich preisgeben. Die meisten Social Media können nicht für die Sicherheit von persönlichen Daten garantieren.

Wie könnte man den Cyberspace sicherer machen?
Wir sollten vor allem die grossen Internet-Firmen dazu drängen, dass sie die Verletzlichkeit ihrer Nutzer und Sicherheitslücken im System effektiv bekämpfen. Denn selbst wenn Internet-Nutzer lernen, sich vorsichtig und bewusst im Internet zu bewegen, haben sie über die Sicherheitslücken der Systeme keine Kontrolle.

«Die meisten Social Media können nicht für die Sicherheit von persönlichen Daten garantieren.»

Wie schwierig ist es für die Polizei gegen Cyberkriminelle vorzugehen?
Die Polizei ist heute noch fast machtlos. Cyberkriminalität hält sich nicht an Staatsgrenzen und die Spuren im Cyberspace können sehr gut verwischt werden. Es ist deshalb enorm schwierig, die Urheber einer Attacke zu eruieren. Die Kriminellen können irgendwo auf der Welt sein und in meinen Computer einbrechen. Zudem getrauen sich Private aus Scham oft gar nicht die Polizei zu kontaktieren. Das wissen die Cyberkriminellen natürlich und nützen dies skrupellos aus.

Ist die Schweiz heute bereits gut auf Cyberattacken vorbereitet?
Nicht wirklich. Zwar steigt das Bewusstsein für die Dringlichkeit des Problems, aber es fehlt an Ressourcen und konkreten Massnahmen. Bisher wurden erst zwei Fälle vor dem Bundesgericht behandelt, obschon wir wissen, dass es viel mehr Delikte gibt.

Waren Sie selbst auch schon Mal Opfer von Cyberkriminellen?
Ja, anfangs 2015 wurden nach den Anschlägen auf die Redaktion der Satire-Zeitschrift «Charlie Hebdo» in Paris viele französischsprachige Webseiten zum Thema Cybersecurity attackiert. Meine Webseite wurde ebenfalls lahmgelegt. Das war beängstigend, denn auch das ist eine Art von Terrorismus. Es hat mich zudem zwei Tage Arbeit gekostet, bis die Webseite wieder lief.

Kritische Infrastrukturen wie etwa Elektrizitäts- und Wasserwerke, Telekomfirmen, Verkehrsbetriebe, aber auch Banken und grosse Spitäler sind zunehmend Ziele von Hackerangriffen.

Kritische Attacken aus dem Internet

Kriminelle Angriffe aus dem Internet haben in den letzten Jahren markant zugenommen. Aufgrund der immer grösseren Vernetzung sind zunehmend auch wichtige Infrastrukturen betroffen. Nicht alle sind gleich gut gegen solche Attacken geschützt.

Ende November 2014 legten zwei unbekannte Gruppen für mehrere Tage das gesamte Firmennetz von Sony Pictures Entertainment lahm. Die Angreifer erklärten, sie wären im Besitz von geheimen Informationen aus dem Unternehmen, und drohten, diese zu publizieren. Tatsächlich tauchten wenig später fünf unveröffentlichte Filme auf Internet-Tauschbörsen auf. Das amerikanische FBI kam später zum Schluss, dass hinter dem Angriff vermutlich die nordkoreanische Regierung stand, welche die Veröffentlichung des Filmes «The Interview» verhindern wollte. Die Filmkomödie handelt von einem Mordkomplott gegen Nordkoreas Staatsoberhaupt Kim Jong-un.

Solche spektakulären grossen Cyber-Angriffe sorgen für viel Aufmerksamkeit in den Medien. Doch sie scheinen, zumindest was man in der Öffentlichkeit weiss, doch immer noch eher die Ausnahme zu sein. Weitaus häufiger sind kleinere, unauffällige Angriffe. Dabei versuchen die Angreifer, möglichst unbemerkt Lücken im Abwehrdispositiv zu finden, um beispielsweise an heikle Informationen zu gelangen oder Gelder von Bankkonten zu stehlen. Perfid ist, dass die Betroffenen häufig erst relativ spät merken, dass sie überhaupt angegriffen werden. Und wenn sie es dann merken, ist es für sie nicht immer leicht zu erkennen, wer hinter den Angriffen steckt.

Gefahren für die Gesellschaft

In den letzten Jahren haben auch die Angriffe auf Industrieanlagen zugenommen. Legendär ist etwa der Angriff mit dem Computerwurm Stuxnet, mit dem 2010 vermutlich die Amerikaner oder Israelis die iranischen Urananlagen gezielt beschädigten. Auch in Deutschland gab es im letzten Jahr einen spektakulären Fall: Bei einem Stahlwerk gelang es unbekannten Angreifern, die Steuerungssoftware eines Hochofens so zu manipulieren, dass dieser stark beschädigt wurde.

Gezielte Angriffe auf technische Anlagen könnten auch die Schweiz treffen. Um unser Land möglichst gut gegen einen solchen Fall zu wappnen, hat der Bund die Fachstelle «Melani» gegründet. Die Experten des Bundes stellen zum einen öffentlich zugängliche Informationen zur Verfügung, wie sich Firmen und Private besser schützen können. Zum anderen arbeitet Melani eng mit den Betreibern kritischer Infrastrukturen zusammen. Dabei handelt es sich um Institutionen, deren Funktionieren für die Gesellschaft unabdingbar ist, etwa Elektrizitäts- und Wasserwerke, Telekomfirmen oder Verkehrsbetriebe, aber auch Banken und grosse Spitäler.

Die einzelnen Branchen seien unterschiedlich gut gegen Angriffe gerüstet, meint Pascal Lamia, Leiter der Fachstelle. Während Banken ihre IT-Infrastruktur heute sehr gut geschützt haben, sehen sich Elektrizitätsunternehmen in einer schwierigeren Lage: Die Strombranche befindet sich im Umbruch, der zu neuen Risiken führt. Laufend werden neue Stromtechnologien ans Netz angeschlossen; gleichzeitig müssen die Firmen sparen.

Schwer beherrschbare Spitäler

Kritisch ist gemäss Lamia die Situation vor allem in Spitälern. Dort hat die Vernetzung in den letzten Jahren rasant zugenommen. Eine Operation kann heute beispielsweise ohne funktionierende IT-Infrastruktur nicht mehr durchgeführt werden. «Das Problem ist, dass in den Spitälern viele Geräte miteinander vernetzt sind, die unterschiedlich funktionieren und unterschiedlich gut geschützt sind. Angesichts des grossen Kostendrucks im Gesundheitswesen ist das für jedes Spital eine grosse Herausforderung.»

Das grösste Risiko sieht Lamia jedoch in einem anderen Bereich, nämlich bei den kleinen und mittleren Unternehmen: Im Gegensatz zu den grossen Firmen sind diese aus personellen und finanziellen Gründen häufig nicht in der Lage, sich genügend gegen Cyber-Angriffe zu schützen. Gerade kleinere Unternehmen werden denn auch immer häufiger von Cyber-Kriminellen erpresst. Die Angreifer drohen beispielsweise einer Firma, die im Internet Produkte verkauft, ihre Webseite würde lahmgelegt, wenn das Unternehmen nicht einen bestimmten Betrag bezahle. Obwohl der Bund dringend davon abrät, solchen Forderungen nachzukommen, weiss Lamia von Firmen, welche die geforderte Summe bezahlt haben, weil der Ausfall der Seite noch höhere Kosten verursacht hätte.

Risikofaktor Smartphone

Das Smartphone rückt immer mehr in unseren Lebensmittelpunkt. Wir senden täglich unzählige Nachrichten über diese mobile Gerät und haben auf diesem praktischen Gerät auch viele persönliche Daten gespeichert – Bilder beispielsweise oder Daten von Gesundheits-Apps. Genau deshalb ist es für jeden Nutzer und jede Nutzerin wichtig, sich zum Thema Datensicherheit Gedanken zu machen. Was geschieht beispielsweise, wenn das Gerät verloren geht oder gestohlen wird? Sind die Daten hoffnungslos verloren? Und was ist, wenn diese Informationen in falsche Hände geraten?

Nicholas Hansen hat bereits zum dritten Mal an der Cyber Security Challenge teilgenommen. Am Schweizer Finale mussten die Teams nicht nur ihre Fähigkeiten auf vielfältige Weise unter Beweis stellen.

▸ Nicholas Hansen: «Wenn man als Hacker Erfolg haben will, muss man ein Gespür entwickeln, wo sich in einem System eine Schwachstelle befinden könnte, und geduldig sein.»

Ein Spiel mit ernstem Hintergrund

Wie schützt man sich gegen Internetattacken? Diese Frage fasziniert Nicholas Hansen. Dass der 19-Jährige in seiner Altersklasse einer der besten Hacker der Schweiz ist, hat er diesen Herbst an der Cyber Security Challenge unter Beweis gestellt.

Zu meinem Lieblingsthema Cyber Security kam ich eigentlich durch Zufall. Im zweiten Lehrjahr als Informatiker hatten wir in der Schule ein Modul über Sicherheit im Internet, und das Gebiet faszinierte mich auf Anhieb. In der Freizeit habe ich mich dann selber mit dem Thema weiterbeschäftigt. Irgendwann machte mich ein Kollege auf die «Cyber Security Challenge» aufmerksam. Das sei doch etwas für mich, meinte er. Und damit hatte er Recht.

Dieses Jahr habe ich bereits zum dritten Mal an diesem Nachwuchswettbewerb teilgenommen, der vom Verein Swiss Cyber Storm organisiert wird. Aufgrund der grossen Teilnehmerzahl verlief die Selektion dieses Mal etwas anders als in den Vorjahren: In der Qualifikationsphase musste zuerst jeder für sich alleine bestimmte Aufgaben lösen. Diejenigen von uns, welche diese Phase erfolgreich bestanden, durften dann Mitte September am Schweizer Finale in Sursee teilnehmen. Dort mussten wir in kleinen Teams knifflige Aufgaben lösen, beispielsweise versteckte Sicherheitslücken in Webanwendungen finden, verschlüsselte Dokumente knacken oder uns einen Zugang zu einem geschützten System verschaffen.

Für die 10 Besten von uns ging es dann nochmals weiter: Wir durften im Oktober im KKL Luzern die Schweiz am Europäischen Finale vertreten. Dort mussten wir uns gegen Teams aus Deutschland, Österreich, England, Spanien und Rumänien behaupten. Jedes Team bestand aus zehn Mitgliedern und hatte einen eigenen Webserver zur Verfügung, auf dem Applikationen mit bestimmten Schwachstellen liefen. Unsere Aufgabe bestand darin, diese Anwendungen zu sichern und die Schwachstellen auszubessern. Gleichzeitig mussten wir versuchen, in die Sever der konkurrierenden Teams einzudringen.

Auf dieses Finale haben wir uns als Team intensiv vorbereitet. Wir haben eine zentrale Ablage eingerichtet, auf der wir alle unsere Tools ablegten, und einen gemeinsamen Chat-Kanal eingerichtet. Wir haben uns klar abgesprochen, wer in unserem Team für was zuständig ist. Ich selbst war dafür zuständig, Angriffe von anderen Teams frühzeitig zu erkennen. Es war jeweils interessant zu sehen, wie die anderen uns angriffen, denn das gab uns Hinweise, auf welchem Weg wir ihre Systeme knacken könnten. Leider hat es nicht für den Sieg gereicht. Wir wurden Dritte.

Mit dem Thema Cyber Security befasse ich mich momentan vor allem in meiner Freizeit. Das Ganze ist für mich eine Art Spiel: Mir macht es grossen Spass, Probleme zu lösen, andere anzugreifen und mich gegen Angriffe geschickt zu verteidigen. Wenn ich eine knifflige Aufgabe gelöst habe, dann gibt mir das ein gutes Gefühl. Und wenn ich mit meinen Ideen vorerst noch nicht durchkomme, dann ist das zwar manchmal etwas frustrierend, aber es spornt mich gleichzeitig auch an. Wenn man als Hacker Erfolg haben will, muss man ein Gespür entwickeln, wo sich in einem System eine Schwachstelle befinden könnte. Wenn ich zum Beispiel auf einer älteren Webseite ein Inputformular sehe, dann interessiert es mich sofort zu sehen, ob die Infrastruktur hinter diesem Formular eine Schwachstelle aufweist. Oder wenn bei einem Programm ein Passwort in verschlüsselter Form abgespeichert wird, möchte ich herausfinden, wo genau das gemacht wird und nach welchem Muster die Verschlüsselung geschieht.

Wenn man als Hacker Erfolg haben will, muss man geduldig sein und immer wieder neue Sachen ausprobieren. Leider vergeht die Zeit in der Regel sehr schnell, und es kommt immer wieder vor, dass ich bis spät in die Nacht hinein vor dem Computer hängen bleibe. Manchmal brauche ich mehrere Tage, bis ich eine Aufgabe gelöst habe. Dann ist es für mich nicht so einfach abzuschalten. Am besten gelingt mir das, wenn ich bei einer guten Idee sofort aufhöre. So komme ich nicht in Versuchung immer länger weiterzumachen.

Im Moment arbeite ich noch bei meiner Lehrfirma. Ich bin als Informatiker für den Betrieb der internen IT-Infrastruktur verantwortlich. Nach der Rekrutenschule werde ich wahrscheinlich ein Informatikstudium in Angriff nehmen. Ich kann mir gut vorstellen, später im Bereich Internetsicherheit zu arbeiten, denn dieser Bereich ist für die Gesellschaft sehr wichtig. Heute werden immer mehr Geräte und Anlagen, die zuverlässig funktionieren müssen, miteinander vernetzt. Und damit steigt natürlich auch die Gefahr, dass sie durch Internet-Angriffe lahmgelegt werden. Wenn wir wissen, wo die Schwachstellen sind, dann können wir diese Anlagen besser schützen.

AHA!

Wie funktioniert eigentlich Verschlüsselung?

Durch Verschlüsseln wird ein so genannter Klartext, also ein normal lesbarer Text, in einen «Geheimtext» umgewandelt, der scheinbar nur Nonsens ist. Schon im alten Ägypten wurden wichtige Nachrichten zu Geheimtexten umgeschrieben, um zu verhindern, dass diese gelesen werden könnten, falls sie bei der Übermittlung in die falschen Hände gerieten. Heute dient Verschlüsselung vor allem der sicheren Übermittlung von Informationen durch digitale Kanäle wie das Internet. So ermöglicht die Verschlüsselung von E-Mails, dass vertrauliche Nachrichten vom Absender an den Empfänger geschickt werden können, ohne dass irgendjemand ausser den beiden diese lesen kann. Dazu braucht es nämlich einen «Schlüssel». Bei modernen, computerbasierten Verschlüsselungsverfahren ist dies eine Bitfolge, also eine sehr lange Zahl bestehend aus Nullen und Einsen. Heute gebräuchliche Verschlüsselungsverfahren bauen auf eine relative Sicherheit. Der Rechenaufwand, um einen Schlüssel zu knacken, soll so gross sein, dass dieser in vernünftiger Zeit und mit üblichen Rechenanlagen nicht geknackt werden kann.

Symmetrisch oder asymmetrisch

Grundsätzlich unterscheidet man zwei Arten von Verschlüsselung: Symmetrische Verschlüsselungsverfahren verwenden zur Ver- und Entschlüsselung denselben geheimen Schlüssel. Bei der asymmetrischen Verschlüsselung hingegen wird zur Verschlüsselung des Klartextes ein anderer Schlüssel als zur Entschlüsselung des Geheimtextes benutzt. Dabei ist der Schlüssel zum Verschlüsseln öffentlich, das heisst, auch anderen Nutzern bekannt. Der Schlüssel zum Entschlüsseln ist dagegen geheim.

Die Kryptologie ist eine Wissenschaft, die sich mit Informationssicherheit beschäftigt. Dazu gehören die Fachgebiete der Kryptographie, die sich mit dem Verschlüsseln befasst, und der Kryptanalyse, die sich dem Knacken von Verschlüsselung widmet.

www.satw.ch/wettbewerb

Ausbildung

Wer Experte oder Expertin im Bereich Cyber Security werden will, braucht gute Informatikkenntnisse. Ausbildungen in Informatik werden in der Schweiz sowohl über Berufslehre und Fachhochschulen wie auch an den meisten Universitäten inklusive ETH Zürich und EPFL angeboten.

Eine Übersicht über die Ausbildungsmöglichkeiten ist zu finden unter
www.berufsberatung.ch > Berufswahl > Berufe und Ausbildungen > Informatik > Suchen

Die Berufsmöglichkeiten generell im Bereich Sicherheit – also auch für Sicherheitsaspekte in der realen Welt – sind sehr vielfältig:
www.berufsberatung.ch > Berufswahl > Berufe und Ausbildungen > Sicherheit > Suchen

Wettbewerb

Was weisst du über die Cyber Security? Teste dein Wissen, mach am Wettbewerb mit und gewinne einen von drei Gutscheinen von Digitec im Wert von 150 Franken. Mit dem Gutschein kannst du zum Beispiel ein Sicherheitsprogramm kaufen, das deinen Computer vor Cyber-Attacken schützt, oder viele andere schöne Dinge. Der Wettbewerb ist bis zum 30. April 2016 offen.
www.satw.ch/wettbewerb

Impressum

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

Konzept und Redaktion: Beatrice Huber
Redaktionelle Mitarbeit: Felix Würsten, Samuel Schläfli
Bilder: Fotolia, Swiss Cyber Storm, Nicholas Hansen, Solange Ghernaouti

Gratisabonnement und Nachbestellungen
SATW, Gerbergasse 5, CH-8001 Zürich
technoscope@satw.ch, Tel +41 (0)44 226 50 11

Technoscope 1/16 erscheint im Mai 2016 zum Thema «Gotthard-Basistunnel».