SKP INFO
DAS MAGAZIN DER SCHWEIZERISCHEN KRIMINALPRÄVENTION
1 | 2021

Thema Cybersicherheit

Cybersicherheit ist S-U-P-E-R.ch

Liebe Leserin, lieber Leser


SKP

Kein Tag vergeht, ohne dass irgendwo in der Schweiz jemand einem Online-Betrug zum Opfer fällt. Zum Beispiel landet eine Phishingmail in unserem Posteingang, in dem wir aufgefordert werden, eine Zahlung zu leisten, um ein Paket zu erhalten. Oder es handelt sich um eine Erpressermail, in welcher gedroht wird, dass jemand angeblich im Besitz von intimen Aufnahmen sei und diese bei Nichtbezahlen eines geforderten Geldbetrages veröffentlichen würde. Auf Fake-Webseiten werden Waren oder Immobilien zu unglaublich attraktiven Preisen angeboten, wobei Namen und Logos von bekannten Unternehmen oder auch Prominente als Lockvögel eingesetzt werden, um betrügerische Angebote seriös wirken zu lassen und so potentielle Opfer in die Falle zu locken. Ganze Firmen und Organisationen werden gehackt und erpresst. Die Liste der Vorgehensweisen könnte hier endlos weitergeführt werden; der Phantasie der Gauner sind und werden praktisch keine Grenzen gesetzt – auch von den Strafverfolgungsbehörden leider nur kaum. Nicht etwa, weil diese nicht wollten, sondern weil sie als nationale Behörden den zumeist international agierenden Kriminellen (noch) nicht viel entgegensetzen können. Deshalb ist in diesen Deliktsbereichen die Prävention besonders wichtig.

So hat sich jetzt die SKP zusammen mit allen Polizeikorps, dem Nationalen Zentrum für Cybersicherheit (NCSC), der Swiss Internet Security Alliance (SISA) und «eBanking – aber sicher!» (EBAS) zusammengetan, um über eine breit angelegte Präventionskampagne die Schweizer Bevölkerung zu erreichen und darauf aufmerksam zu machen, wie sich jede und jeder im Internet einfach, aber effektiv schützen kann: nämlich mit den «5 Schritten für Ihre digitale Sicherheit».

Erfahren Sie in dieser Ausgabe mehr über die Hintergründe zu diesem gemeinsamen Projekt und mehr über die Behörden und Organisationen, die sich alle der Prävention von Cyberdelikten verschrieben haben: Die NCSC stellt ihre Neuausrichtung und die allgemeinen Schwerpunkte vor. Die SISA ist ein Verein mit Schweizer Wirtschafts- und Behördenvertretern, welcher mit seiner Online-Marke «iBarry.ch» eine digitale Plattform zur Internetsicherheit betreibt. EBAS ist ebenfalls eine unabhängige Plattform (ein Produkt der Hochschule Luzern) und tritt im Namen von Schweizer Finanzinstituten auf. Die mit der Umsetzung der Ideen beauftragte Agentur nimmt im Interview Stellung, welche Erfahrungen sie mit diesem Auftrag und den Auftraggebern gemacht haben. Ausserdem stellt NEDIK (das Netzwerk der Polizeibehörden zur Ermittlungsunterstützung gegen die digitale Kriminalität) die Neuausrichtung im Bereich Prävention Cybercrime vor. Und schliesslich wird von der SKP zusammen mit «Ihrer Polizei» kurz erklärt, warum wir dieses gemeinsame Projekt durchführen.

Falls wir Sie nun «gluschtig» gemacht haben und Sie nun wissen wollen, was in dieser Kampagne vom 3. – 7. Mai 2021 genau passieren wird, folgen Sie unseren Social-Media-Kanälen. Am 3. Mai geht's los!

Ich wünsche Ihnen eine anregende Lektüre!

Fabian Ilg

Stellvertretender SKP-Geschäftsleiter und Projektverantwortlicher Cybercrime

IMPRESSUM

Herausgeberin und Bezugsquelle
Schweizerische Kriminalprävention
Haus der Kantone
Speichergasse 6
Postfach
3001 Bern

info@skppsc.ch
Tel. 031 511 00 09

Das **SKP INFO 1 | 2021** ist als PDF-Datei zu finden unter: www.skppsc.ch/skpinfo. Es erscheint auch in französischer und italienischer Sprache.

Verantwortlich		Chantal Billaud, Geschäftsleiterin SKP
Redaktion		Volker Wienecke, Bern
Übersetzungen	**F**	ADC, Vevey
	I	Annie Schirrmeister, Massagno
Layout		Weber & Partner, Bern
Druck		Länggass Druck AG, Bern
Auflage		D: 1350 Ex. | F: 300 Ex. | I: 250 Ex.
Erscheinungsdatum		Ausgabe 1 | 2021, April 2021

Aktionswoche zur digitalen Sicherheit: Cybersicherheit ist S-U-P-E-R!

Mit einer Aktionswoche vom 3. bis am 7. Mai 2021 will die Schweizerische Kriminalprävention gemeinsam mit weiteren Organisationen die Bürgerinnen und Bürger für die digitale Sicherheit sensibilisieren. Die Kampagne ist digital ausgelegt und soll überraschen, interessieren und informieren. Ein mehrstufiges Angebot sorgt dafür, dass sich niemand über- oder unterfordert fühlt und dass möglichst alle einen Mehrwert haben. SKP-Projektleiterin Beatrice Kübli erklärt, warum das S-U-P-E-R ist und was dahintersteht.

zvg

S-U-P-E-R dient als Merksatz für die fünf Schritte zur digitalen Sicherheit und ist auch die URL für die Landingpage der Kampagne.

Autorin

Beatrice Kübli
Projektleiterin bei der Schweizerischen Kriminalprävention

SKP

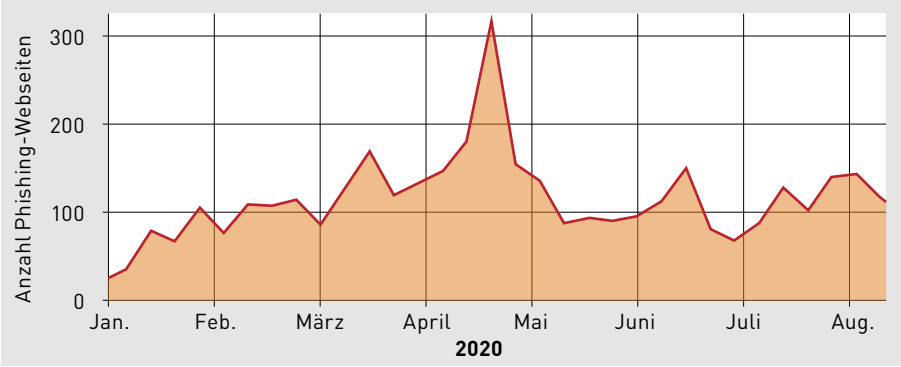
Wer kennt das nicht: Der Zahnarztbesuch steht an und man ahnt bereits, jetzt kommt wieder die Frage, wie oft man die Zahnseide benutzt habe? Klar weiss man, dass das wichtig wäre, aber eben … So ähnlich ist das bei vielen Präventionsthemen, eben auch bei der digitalen Sicherheit. Oder haben Sie kürzlich ein Backup von Ihren privaten Daten gemacht? Meist reicht ein Anstoss von aussen, um aktiv zu werden, das Pech des Kollegen beispielsweise, dem das Laptop in die Aare gefallen ist und der dabei seine ganze Fotosammlung verloren hat. Da wir niemandem wünschen, dass die Fotosammlung (oder noch Wichtigeres!) den Fluss ab geht, übernehmen wir diesen «Anstoss von aussen» mit einer Aktionswoche.

«Wir» – das sind die SKP gemeinsam mit den Polizeikorps unter «Ihre Polizei», das Nationale Zentrum für Cybersicherheit NCSC, die Swiss Internet Security Alliance SISA mit der Plattform «iBarry» und die Plattform «eBanking – aber sicher!» (EBAS) der Hochschule Luzern. In der Sensibilisierungskampagne vom 3. bis am 7. Mai 2021 zeigen wir den Bürgerinnen und Bürgern in fünf Schritten, wie sie ihre Daten und Internetzugänge schützen können. Realisiert wird die Kampagne von der Agentur «Partner & Partner» aus Winterthur.

«Warum wird ausgerechnet die digitale Sicherheit thematisiert?», könnte man sich fragen. Schliesslich gibt es in der Präventionslandschaft auch andere wichtige Themen, für welche man die Bevölkerung sensibilisieren sollte. Um es gleich vorwegzunehmen: Wir können uns vorstellen, die Aktionswoche zukünftig regelmässig und auch zu anderen Themen durchzuführen. Dass wir mit der digitalen Sicherheit beginnen, hat aber gute Gründe.

Prävention ist einfacher als Ermitteln

Das Internet bietet für Kriminelle zahlreiche Möglichkeiten, zu betrügen und sich zu bereichern: Computer können von den Besitzerinnen und Besitzern unbemerkt zu kriminellen Zwecken eingesetzt werden, manche Angreiferinnen und Angreifer haben es auf private Daten wie Bank-Logins abgesehen, einige stehlen ganze Identitäten oder sperren den Zugang zu den Daten des Opfers. Die Ermittlungen sind schwierig und oft wenig ergiebig, denn die Täterinnen und Täter agieren aus



Gemeldete und bestätigte Phishing-Webseiten pro Woche auf antiphishing.ch im ersten Halbjahr 2020[1]

dem Ausland und nutzen die Möglichkeiten des Internets zur Anonymisierung ihrer Identität und zur Verschleierung der Aktivitäten. Ermittlungen und Fahndungen erfordern eine internationale Zusammenarbeit, was nicht mit allen Ländern einfach zu bewerkstelligen ist, sowie fundierte Informatikkenntnisse und die entsprechende Infrastruktur. Cyberdelikte machen einen immer grösseren Anteil der Straftaten aus, wobei Cyberbetrug und Phishing überwiegen. Über die Hälfte der Meldungen beim fedpol betrafen in den letzten Jahren diese beiden Deliktformen.[2] Auch bei der Meldestelle des NCSC wurden im ersten Halbjahr 2020 wöchentlich rund 100 Phishing-Seiten gemeldet.

Aber längst nicht alle Opfer von Cyberangriffen melden sich bei der Polizei. Die einen schämen sich, dass sie auf so einen Betrug hereingefallen sind. Andere resignieren, glauben nicht an eine Aufklärung des Deliktes und erheben deswegen auch keine Anzeige. Die Dunkelziffer ist hoch, und der persönliche und wirtschaftliche Schaden beachtlich. Es lohnt sich daher gerade bei der digitalen Sicherheit, auf Prävention zu setzen. Mit wenigen, recht einfachen Mitteln kann viel vermieden werden. Wer sichere Passwörter verwendet, regelmässig seine Software aktualisiert und einen Virenschutz installiert hat, riskiert weniger, Ziel eines Cyberangriffs zu werden. Wichtig ist überdies auch, dass sich die Bürgerinnen und Bürger der Gefahren bewusst werden und dubiose E-Mails oder Kurznachrichten kritisch hinterfragen. Wer weiss, wie ein Phishing- oder Hacking-Angriff funktioniert, lässt sich von scheinbar dringenden Meldungen weniger zu einer unüberlegten Handlung hinreissen und fällt auch nicht auf jedes gar so tolle Angebot herein. Steigt das Gefahrenbewusstsein der Einzelnen, so schützt dies auch die Unternehmen vor grösseren Angriffen, denn auch im beruflichen Rahmen wird er/sie nicht mehr auf jeden interessanten Link klicken. Zwar gibt es auch Hackerangriffe, die rein technisch ablaufen, meist setzen die Delinquenten aber auf die «Schwachstelle Mensch». Und hier setzen wir mit unserer Kampagne an.

Eine Woche – das ist machbar!

Die ursprüngliche Idee der Kampagne war es, eine Art digitalen Frühlingsputz zu machen. Bei so einer Aktion werden die Dinge mal wieder in Ordnung gebracht, und Pendenzen, die schon länger anstehen, werden erledigt. Die Idee des Putzens schien uns dann für die Thematik doch nicht ganz passend, geht es doch eher um Sicherheit als um Sauberkeit. Aber der Grundgedanke einer Aktionswoche blieb: eine Woche lang mitmachen und die Dinge in Ordnung bringen. Die «Fünf Schritte zur digitalen Sicherheit», die wir bereits 2020 gemeinsam mit EBAS erarbeitet hatten, boten sich für eine Wochenaktion an. An jedem Wochentag präsentieren wir einen Schritt. Eine Woche ist überschaubar, und das erhöht die Motivation mitzumachen. Zudem erhoffen wir uns einen hohen Impact, wenn wir die geballte Kraft dieser Kampagne auf eine Woche fokussieren können.

Mit der Kampagne wollen wir in erster Linie die Bürgerinnen und Bürger für die Wichtigkeit der digitalen Sicherheit sensibilisieren. Es soll klar werden, dass auch digitale Geräte, sei es nun Computer, Tablet oder Handy, geschützt werden müssen und dass jeder selbst Verantwortung für seine digitale Sicherheit übernehmen muss und auch kann. Danach braucht es natürlich das Wissen, wie man sich und seine Geräte schützen kann und wie man einen Angriff erkennt. Und schliesslich muss man dieses Wissen auch umsetzen können. Diese Dreistufigkeit nehmen wir in der Kampagne auf.

Bewusstsein schaffen

Das Wichtigste einer Präventionskampagne ist, dass die Leute sie wahrnehmen. Die besten Plakate und Posts nützen nichts, wenn keiner hinschaut. In dieser Kampagne setzen wir dazu auf Humor und Überraschung. Es war uns zudem wichtig, dass gleich beim ersten Blick der Bezug zum Thema hergestellt wird, so dass jeder sofort versteht, um was es geht. Die Agentur hat dazu fünf Sujets entworfen: Man sieht jeweils ein Gerät, mal einen Computer, ein Tablet oder Handy, kombiniert mit etwas, das man im Alltag mit «Sicherheit» in Ver-

1 Quelle: Nationales Zentrum für Cybersicherheit NCSC/MELANI: «Informationssicherung. Lage in der Schweiz und International. Halbjahresbericht 2020/I (Januar–Juni)», 29. Oktober 2020, online: www.ncsc.admin.ch → Dokumentation → Berichte → Lageberichte → Halbjahresbericht 2020/1

2 National Risk Assessment (NRA): «Betrug und Phishing zwecks betrügerischen Missbrauchs einer Datenverarbeitungsanlage als Vortat zur Geldwäscherei Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT)», Januar 2020, online: www.sif.admin.ch → Finanzmarktpolitik und -strategie → Integrität des Finanzplatzes → Berichte

bindung bringt. Die Kombinationen kommen real nicht vor, was Verblüffung, Überraschung und Irritation erzeugt und witzig wirkt. Da schwimmt etwa ein Laptop im Rettungsring, und auf dem Tablet hat es Zahnpasta. Auch wer nur kurz hinschaut, nimmt so intuitiv die Botschaft «digitale Geräte schützen» auf. Wer länger hinschaut, kann etwas lernen.

Wissen aufbauen

Die Sujets werden begleitet von einem kurzen Spruch, der erklärt, was das Bild mit Cybersicherheit zu tun hat. Jedes Sujet bezieht sich auf einen der fünf Schritte. Beim Bild mit dem Rettungsring steht dazu «Sichern Sie Ihre Daten, bevor sie abtauchen.» Dadurch wird auf eine einfache und zugängliche Weise vermittelt, dass Datensicherungen ein Schritt zur digitalen Sicherheit sind. Damit man sich die fünf Schritte besser merken kann, hat die Agentur ein Merkwort geschaffen, und das ist S-U-P-E-R! Wirklich! S wie Sichern, U wie Updaten, P wie Prüfen, E wie Einloggen und R wie Reduzieren. Dies ist dann auch die URL zur Website, wo es weitere Informationen und Handlungsanweisungen gibt.

zvg

Datensicherung ist einer der fünf Schritte zur digitalen Sicherheit. Jeder Schritt wird mit einem eigenen Sujet illustriert.

Handlungskompetenz vermitteln

Wer mehr darüber erfahren möchte, wie er sich und seine Geräte im Internet schützen kann, findet auf der Projekt-Landingpage detaillierte Informationen und Erklärungen dazu, wie die einzelnen Schritte umgesetzt werden können. Jeder Schritt wird mit einem kleinen Text erklärt. Wer sich in ein Thema vertiefen möchte, kommt via Links zu den Partnerorganisationen, wo alles ausführlich erklärt wird, oder kann eines der vom NCSC angebotenen Webinare besuchen.

Dieses mehrstufige Angebot an Informationen erlaubt es, die Bürgerinnen und Bürger dort abzuholen, wo sie stehen. Wer schon viel weiss, kann sich via Landingpage Expertenwissen holen, wer noch nicht viel davon versteht, findet einen einfachen und niederschwelligen Zugang zum Thema.

Verbreitung via Netzwerkpower

Für die breite, schweizweite Streuung der dreisprachigen Kampagne setzen wir auf unsere Netzwerke. Dass die Inhalte von möglichst vielen Partnern gestreut werden, ist zentral für den Erfolg dieser Kampagne. Die Polizeikorps sowie verschiedene Banken haben ihre Beteiligung bereits zugesichert, diverse Wirtschaftspartner von SISA sind interessiert. Die Koordination aller Beteiligten ist eine Herausforderung, aber für die SKP nichts Neues. Wir haben bereits sehr gute Erfahrungen mit unserem Netzwerk gemacht und sind zuversichtlich, dass es auch bei dieser Aktionswoche zuverlässig funktionieren wird. Nun gilt es, auch der Gesellschaft zu zeigen, wie gut vernetzt wir sind: Bei dieser Aktion geht es nicht nur um die digitale Sicherheit. Es geht auch darum, die Polizei und die Mitgliedsorganisationen als kompetente Ansprechpersonen zu positionieren und zu zeigen, wie vielschichtig und koordiniert das Schweizer Netzwerk Cybersicherheit funktioniert. Das wird sicher S-U-P-E-R!

«eBanking – aber sicher!»

Die Dienstleistung «eBanking – aber sicher!» (EBAS), welche vom Departement Informatik der Hochschule Luzern angeboten wird, unterstützt Schweizer Bürgerinnen und Bürger sowie Bankmitarbeitende rund um das Thema IT-Sicherheit mit dem Fokus E-Banking.

Im April 2017 nahm ich an einer Präventionsveranstaltung bei der Zuger Polizei teil und kam während des anschliessenden Aperitifs (ja, das war in der Vor-Corona-Zeit noch gang und gäbe) mit dem Zuger Cyberermittler ins Gespräch und auf die Schweizerische Kriminalprävention (SKP) zu sprechen. Ich sah sofort grosses gegenseitiges Potenzial, und da der Zuger Cyberermittler bereits mit der SKP zusammengearbeitet hatte, konnte er mir im Anschluss an die Veranstaltung den Kontakt vermitteln.

Im Juni traf man sich am neu gegründeten Departement Informatik der Hochschule Luzern in Rotkreuz. Eine Auslegeordnung der Engagements der Schweizerischen Kriminalprävention und von «eBanking – aber sicher!» brachte schnell mögliche Zusammenarbeitsmöglichkeiten zu Tage. Im Fokus standen die für andere Präventionsbereiche bereits sehr beliebten und etablierten SKP-Broschüren und -Faltblätter.

Autor

zvg

Oliver Hirschi

Informatiker, ist seit 2013 Dozent für Informationssicherheit an der Hochschule Luzern und dort u.a. mit der Leitung der Dienstleistung «eBanking – aber sicher!» (www.ebas.ch) beauftragt. Er ist Mitautor des «Informationssicherheitshandbuchs für die Praxis» (www.sihb.ch) und Mitglied der Sicherheitsgruppe Schweiz SGRP (www.sgrp.ch).

So entstand bereits im Verlaufe des Herbsts/Winters 2017 die erste gemeinsam erstellte Broschüre zum Thema «5 Schritte für Ihre digitale Sicherheit». Viele weitere folgten, und so sind bis heute sieben Faltblätter in SKP-EBAS-Kooperation entstanden:

- 5 Schritte für Ihre digitale Sicherheit
- Als «Money Mule» für Kriminelle arbeiten?
- Phishing
- Betrügerische Supportanrufe
- Mobile Banking und Mobile Payment
- Sicher auf Social Media
- Rendite genial? Verlust total!

Die Broschüren und Faltblätter werden nicht nur durch die SKP verteilt, sondern auch durch EBAS, direkt im Rahmen von Schulungen, Kursen und Veranstaltungen, aber auch indirekt über die «eBanking – aber sicher!»-Partnerbanken.

Zurück in die unmittelbare Zukunft: Vom 3. bis zum 7. Mai 2021 findet, initiiert durch die Schweizerische Kriminalprävention, eine schweizweite Aktionswoche zur Cybersicherheit statt. Inhaltlich schliesst sich hierbei der Kreis zur ersten gemeinsam erstellten Broschüre, indem die Kampagne pro Tag einen der «5 Schritte für Ihre digitale Sicherheit» ins Zentrum stellt. Wir freuen uns sehr, diese Kampagne als eine von vier Trägerorganisationen mitentwickelt zu haben und lancieren zu können, und natürlich auch auf eine weitere lange und fruchtbare Zusammenarbeit – ganz im Sinne der Prävention und Sensibilisierung der Schweizer Bevölkerung für Cybergefahren.

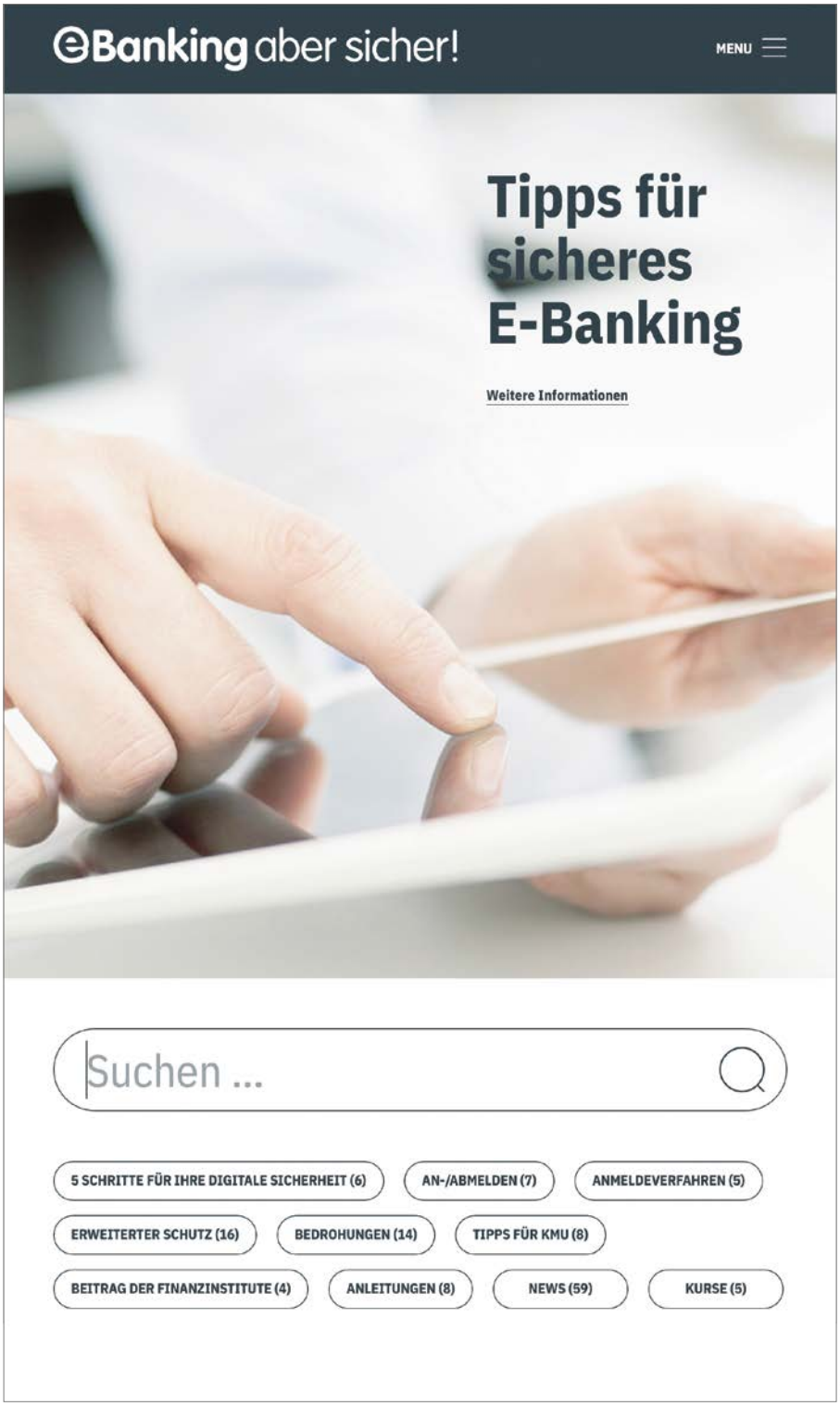
Über «eBanking – aber sicher!»

«eBanking – aber sicher!» (EBAS) ist eine schweizweite Awareness-Kampagne, welche seit über zehn Jahren die Schweizer Bevölkerung sowie Mitarbeitende des Finanzsektors erfolgreich für sicheres E-Banking sensibilisiert. Gestartet im Jahr 2009 mit drei Pilot-Partnerbanken (Credit Suisse, PostFinance und Zürcher Kantonalbank), wird die Kampagne heute von knapp 50 Partnerbanken aus der ganzen Schweiz unterstützt. Die Sensibilisierung baut mehrsprachig auf vier Grundpfeiler auf:

1. Webseite
(Public Service, öffentlich zugänglich)
Damit Frau und Herr Schweizer ihre digitalen Geräte auf einen hohen Sicherheitsstand bringen und dort halten können, benötigen sie Tipps und Hilfestellungen. Diese Unterstützung hat auch zum Ziel, die Benutzer zu einem sicherheitsbewussten Verhalten während der E-Banking-Sitzung anzuleiten.

Die Hochschule Luzern, Departement Informatik stellt auf der Webseite www.ebas.ch konkrete und praxisnahe Informationen zu grundlegenden Sicherheitsmassnahmen und Verhaltensregeln für eine sichere Anwendung digitaler Geräte mit Fokus E-Banking zur Verfügung.

2. Kurse für Endkunden
(Public Service, öffentlich zugänglich)
Über die Webseite werden jährlich leichtverständliche, öffentliche Kundenkurse für verschiedene Zielgruppen angeboten. Das Angebot an verschiedenen Standorten in der ganzen Schweiz reicht von einem Grundkurs und einem Praxiskurs mit Übungen an bereitgestellten Geräten über einen speziellen Online-Kurs für Unter-30-Jährige bis hin zum Kurs für KMU. Der Grundkurs beispielsweise dauert 2½ Stunden und beinhaltet Informationen zu allgemei-



zvg

Auf der Webseite www.ebas.ch der Hochschule Luzern finden Sie konkrete und praxisnahe Informationen zu grundlegenden Sicherheitsmassnahmen und Verhaltensregeln.

nen Sicherheitsfragen und insbesondere zur Sicherheit beim E-Banking. Das aktuelle Kursangebot ist zu finden unter www.ebas.ch → Kurse

3. Medien-Monitoring
(nur für Mitgliedsinstitute)
Medien haben einen grossen Einfluss auf das Sicherheitsgefühl und das Verhalten der Endbenutzer. Entsprechende Berichte über E-Banking können stark verunsichern und viele Fragen aufwerfen, die dann durch den Kundendienst oder die Endkundenberatenden beantwortet werden müssen. Ein zeitnahes Monitoring der Schweizer Medienlandschaft, die Ausarbeitung von entsprechenden Stellungnahmen zuhanden des Helpdesks und der Endkundenberatenden sowie eine Datenbank über die publizierten Berichte und Stellungnahmen steigern die Dienstleistungsqualität deutlich.

Die Hochschule Luzern überwacht in Zusammenarbeit mit der Argus Presse AG die Schweizer Medienberichterstattung (Zeitungen, Online-Medien, Radio und TV) täglich. Alle Artikel rund um die Themen E-Banking und IT-Sicherheit werden gesammelt. Zu jedem relevanten Bericht werden Stellungnahmen verfasst und den Mitgliedsbanken zur Verfügung gestellt. So können auch Bankkundenanfragen zu Sicherheitsthemen durch die Bankmitarbeitenden fundiert und kompetent beantwortet werden.

4. Schulungen für Kundendienstmitarbeitende
(nur für Mitgliedsinstitute)
Endkundenberatende und Mitarbeitende des Helpdesks benötigen rund um das Thema der Informationssicherheit genügend Kompetenz, um Kunden bei allfälligen Fragen professionell zu beraten. Die Hochschule Luzern bietet den Finanzinstituten ein bedürfnisorientiertes Schulungspaket zur Ausbildung von Endkundenberatenden und Helpdesk-Mitarbeitenden.

Summa summarum: Die Website wird aktuell monatlich von knapp 40 000 Besuchenden aufgerufen, und über 1200 Mitarbeitende der beteiligten Finanzinstitute sowie über 4800 Personen wurden bis heute in EBAS-Schulungen und -Kursen für sicheres E-Banking ausgebildet.

Weitere Informationen unter: www.ebas.ch

Sensibilisierung für Cyberrisiken als wichtige Aufgabe des NCSC

Die Cybersicherheit spielt eine zentrale Rolle in der nationalen und internationalen Aussen- und Sicherheitspolitik und ist auch ein wichtiger Faktor für den Wirtschaftsstandort Schweiz. Das Nationale Zentrum für Cybersicherheit (NCSC) ist die erste Anlaufstelle für Privatpersonen, Wirtschaft, Bildungseinrichtungen und Verwaltung, wenn es um den Schutz vor Cyberrisiken geht.

Das NCSC wird vom Delegierten des Bundes für Cybersicherheit, Florian Schütz, geleitet und ist unter anderem zuständig für die koordinierte Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS). Die NCS gibt die Ziele und Massnahmen vor, die wesentlich von Akteuren aus den Kantonen, der Wirtschaft, der Gesellschaft und den Hochschulen mitgetragen werden. Die Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV) bildet ihrerseits die rechtliche Grundlage für den Auf- und Ausbau des NCSC. Sie regelt Struktur, Aufgaben und Kompetenzen der beteiligten Behörden und bildet auch die Grundlage für die Sensibilisierungs- und Präventionstätigkeiten im Bereich der Cyberrisiken[1]. Gerade auf diesem Gebiet sind die Zusammenarbeit und der Austausch inner- und ausserhalb der Bundesverwaltung für das NCSC zentral.

Autorin

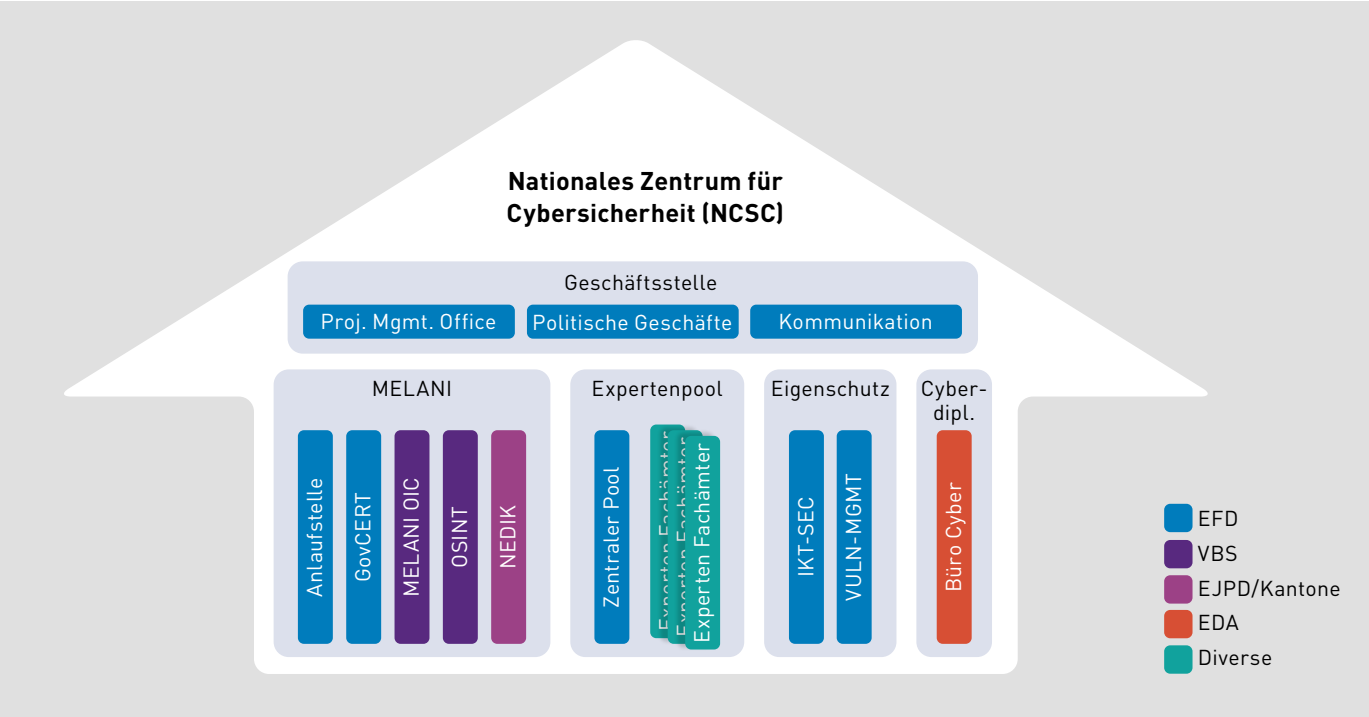
Dominique Trachsel
lic.phil., MAS, MSc FCCI, Verantwortliche Sensibilisierung und Prävention NCSC

zvg

Sensibilisierung und Prävention im NCSC

Cybersicherheit liegt in der Verantwortung eines und einer jeden Einzelnen. Es gehört daher zu den Aufgaben des NCSC, die Öffentlichkeit gezielt über Cyberrisiken zu informieren, um sie für Risiken im Cyberraum zu sensibilisieren. Dabei arbeitet das NCSC eng mit bundesinternen und -externen Stellen zusammen. Gemeinsam werden Anleitungen für präventive Massnahmen erarbeitet und Empfehlungen gegeben für den Fall, dass jemand Opfer eines Cyberdelikts geworden ist. Dementsprechend unterstützt das NCSC die von der Schweizerischen Kriminalpräven-

1 Art. 12 Buchstabe h) Cyberrisikenverordnung



Quelle: NCSC

tion (SKP) initiierte nationale Aktionswoche, die zum Ziel hat, einem breiten Publikum konkrete Massnahmen an die Hand zu geben, um sich sicher und geschützt in der digitalen Welt zu bewegen. Die Aktionswoche wird finanziert und partnerschaftlich getragen von der unabhängigen Plattform «eBanking – aber sicher!» der Hochschule Luzern, der Swiss Internet Security Alliance (SISA/iBarry), der SKP und dem NCSC.

Organisation des NCSC

Das NCSC ist in verschiedene Bereiche gegliedert und umfasst die Geschäftsstelle, die Melde- und Analysestelle Informationssicherung (MELANI), den Expertenpool, den Eigenschutz sowie die Cyberdiplomatie.

MELANI besteht seit 2004 und wurde 2020 mit dem nationalen Computer Emergency Response Team (GovCERT) als technische Fachstelle in das NCSC integriert und weiter ausgebaut. Die Abteilung unterhält zudem die Schnittstellen zum Nachrichtendienst und der Strafverfolgung, um den Informationsfluss zu den aktuellen Bedrohungen sicherzustellen. Die Nationale Anlaufstelle ist ebenfalls in diesen Bereich integriert. Sie nimmt Meldungen zu Cybervorfällen aus der Bevölkerung und der Wirtschaft entgegen, analysiert sie und gibt den Meldenden eine Einschätzung zum Vorfall sowie Empfehlungen für das weitere Vorgehen.

Weiter stellt das NCSC einen Expertenpool zur Verfügung. Die Experten unterstützen die Fachämter bei der Entwicklung und der Umsetzung von Standards zur Cybersicherheit. Hier ist auch der Bereich «Sensibilisierung und Prävention» angegliedert.

Im Rahmen des Eigenschutzes der Bundesverwaltung erlässt das NCSC Vorgaben zur Cybersicherheit, überprüft ihre Einhaltung und unterstützt die Leistungserbringer bei der Beseitigung von Schwachstellen. Ebenfalls auf Stufe Bund entwickelt das «Vulnerability Management» Prozesse und Hilfsmittel und erstattet Bericht über die entdeckten IT-Schwachstellen.

Schliesslich stellt das Cyberbüro des Eidg. Departements für auswärtige Angelegenheiten (EDA) die Zusammenarbeit und die Koordination mit der schweizerischen Aussenpolitik sicher.

Weitere Informationen unter: ncsc.admin.ch

Swiss Internet Security Alliance – ein gemeinnütziger Verein zum Schutz vor Gefahren aus dem Internet

In der Swiss Internet Security Alliance (SISA) treffen sich Vertreter aus Wirtschaft und Behörden, um gemeinsam Cyber-Prävention zu betreiben. Mit dem Betrieb von ibarry.ch stellt die SISA eine umfassende Cyber-Präventions-Webseite zur Verfügung; eine Webseite, auf die auch Polizeikorps im Rahmen ihrer Präventionsbemühungen verweisen können.

Die Schweiz soll das sicherste Internetland der Welt werden

Die Swiss Internet Security Alliance, kurz SISA, wurde 2014 von namhaften Vertretern der Wirtschaft ins Leben gerufen. Mit dabei waren unter anderen die grossen Internet-Provider der Schweiz, welche vereinbart haben, sich nicht konkurrenzieren zu wollen, wenn es darum geht, die Bevölkerung vor Gefahren im Umgang mit dem Internet zu schützen. Die Schweiz zum sichersten Internetland der Welt zu machen, ist denn auch die erklärte Vision der SISA. Entsprechend liegt der Zweck des Vereins darin, die Bevölkerung über Risiken und Problemlösungen in Bezug auf Schwachstellen ihrer mit dem Internet verbundenen Geräte aufzuklären und sie für mögliche Gefahrenpotentiale zu sensibilisieren. Kurz gesagt geht es darum, Cyber-Prävention zu betreiben.

Autor

zvg

Daniel Nussbaumer ist seit 2019 Präsident der Swiss Internet Security Alliance. Zuvor war er vier Jahre lang Chef Cybercrime der Kantonspolizei Zürich und leitete das interkantonale polizeiliche Netzwerk NEDIK, welches gesamtschweizerisch für die Strafverfolgung und die Prävention im Bereich Cyberkriminalität zuständig ist.

Cyber-Prävention ist Knochenarbeit – Nutzen wir Synergien!

Cyber-Prävention ist Knochenarbeit. Das Erstellen und Verbreiten von Präventionskampagnen, die Entwicklung und der Unterhalt von Webseiten oder auch das Vorbereiten und Halten von Referaten erfordert Ressourcen. Ressourcen, für die manch ein Unternehmen und manch eine Behörde Verständnis hat, die im Gesamtkontext jedes Firmenzwecks aber regelmässig nur schwer erhältlich sind.

Auf der anderen Seite wird das Volumen der Cyberkriminalität weltweit auf rund 600 Milliarden Dollar jährlich geschätzt, womit mit Cybercrime mehr Geld umgesetzt wird als im Drogenhandel. Mit anderen Worten: Im Bereich der Cyber-Prävention kämpfen Behörden und Wirtschaft gegen eine 600-Milliarden-Dollar-Industrie.

Entsprechend sinnvoll ist es, Synergien in diesem Bereich zu nutzen, die Arbeiten nicht doppelt und dreifach zu machen, sondern erarbeitete Inhalte und Produkte miteinander auszutauschen und – im besten Fall – Strategien, Kampagnen und Homepages gemeinsam zu entwickeln und aufeinander abgestimmt umzusetzen.

Public Private Partnership

Heute treffen sich in der SISA nicht nur Vertreter aus Wirtschaft, sondern auch aus Behörden und Hochschulen. Als gemeinnütziger Verein bietet die SISA ihren Mitgliedern und Partnern somit die Gelegenheit, gemeinsam Präventionsprodukte zu entwickeln und zu verbreiten.

Die SISA macht dies im Wesentlichen auf zwei Arten. Zum einen unterhält die SISA ein Advisory Board, in welchem sich Mitglieder und Partner der SISA treffen, um gemeinsam Präventionsinhalte zu entwerfen. Zum andern betreibt die SISA die Plattform ibarry.ch, auf welcher zu sämtlichen aktuellen Cyberphänomenen konkrete Verhaltenstipps und Ratschläge für die Bevölkerung vorhanden sind. Ausserdem finden sich auf der Webseite Tools, mit welchen Bürgerinnen und Bürger kostenlos überprüfen können, wie gut ihr Computer vor Cyberangriffen geschützt ist.

Das Advisory Board

Das Advisory Board besteht aus Awareness-Spezialisten der Mitglieder und Partner der SISA. Es ist eine Plattform, in der Präventionsinhalte für konkrete Kampagnen gemeinsam entwickelt werden. Die entsprechenden Präventionsbotschaften sollen dabei so aufeinander abgestimmt sein, dass sämtliche Partner bei der Verbreitung der Präventionsbotschaften dasselbe Wording verwenden.

Zurzeit sind am Advisory Board Vertreter/innen der Internetprovider, von Finanzinstituten, der Behörden und Hochschulen beteiligt. Sie stellen so eine gemeinsame Entwicklung der Präventionsbotschaften zwischen Privaten und Behörden sicher und damit auch die Koordination der Präventionsbemühungen.

Die SISA selbst lanciert inzwischen mindestens vier am Advisory Board entwickelte Awareness-Kampagnen jährlich. Damit leistet die SISA einen wesentlichen – und vor allem mit allen Partnern abgestimmten – Beitrag zur Sensibilisierung der Bevölkerung.

ibarry.ch – eine Plattform für die Präventionsarbeit der Polizeikorps

Cyberangriffe werden immer komplexer und immer vielfältiger. Sie richten sich gegen Menschen und/oder digitale Schwachstellen. Immer häufiger aber stellen Cyberkriminelle mit immer neuen Methoden die Täuschung des Menschen ins Zentrum ihres Angriffes. Ein Beispiel dafür sind E-Mails mit Links oder Anhängen, die dazu führen, dass, wenn sie irrtümlicherweise angeklickt bzw. geöffnet werden, sich Schadsoftware auf dem Computer installieren kann. Andere Beispiele sind Betrugsmails, beispielsweise in Form von Love-Scams oder CEO-Frauds. Neben solchen Angriffen gegen Menschen werden auch Schwachstellen bei der Technik von digitalen Geräten ausgenutzt, um so in diese einzudringen.

So vielfältig Cyberangriffe sind, so schwierig ist es, die Bevölkerung durch gezielte Präventionsmassnahmen vor solchen Angriffen zu schützen. Entsprechend vielfältig fallen die Präventionsmassnahmen aus. Entsprechend aufwändig und ressourcenintensiv ist auch deren Erarbeitung.

Die SISA hat im Jahr 2019 die Marke ibarry.ch ins Leben gerufen. ibarry.ch ist eine umfassende Cyberpräventions-

zvg

seite und enthält zu sämtlichen aktuellen Cyberthemen konkrete Verhaltenstipps. Die Seite wird laufend betreut und aktualisiert. Mit dem Betrieb dieser Seite finanzieren die Mitglieder der SISA eine umfassende Awareness-Plattform für die Schweizer Bevölkerung. Damit können andere Institutionen davon entlastet werden, ihrerseits Ressourcen in die Entwicklung von weiteren Homepages zu investieren, um Vergleichbares nochmals zu tun. Damit haben private Unternehmen oder Institutionen wie beispielsweise Polizeikorps die Möglichkeit, anstatt

aufwändig eigenes Präventionsmaterial zu entwerfen, auf ibarry.ch zu verweisen.

Nationale Kooperation – 5-Schritte-Kampagne im Mai

Zusätzlich zu ihren obgenannten Aktivitäten beteiligt sich die SISA auch an der kommenden 5-Schritte Kampagne, welche die SKP, das NCSC, die SISA und EBAS gemeinsam entwickelt haben und im Mai gemeinsam lancieren werden. Auch diese Zusammenarbeit entstand vor dem Hintergrund, dass wir mehr Wirkung erzielen können, wenn Wirtschaft und Behörden ihre Ressourcen zusammenlegen und gemeinsam auftreten. Wir alle, seien es Internetprovider, Finanzinstitute, Hochschulen oder Behörden, haben das gemeinsame Interesse, die Bevölkerung auf die Gefahren aus dem Internet aufmerksam zu machen und ihr konkrete Verhaltenstipps im Umgang mit dem Internet zu geben. Mit Umsetzung der 5-Schritte-Kampagne tragen wir genau dieser Absicht Rechnung.

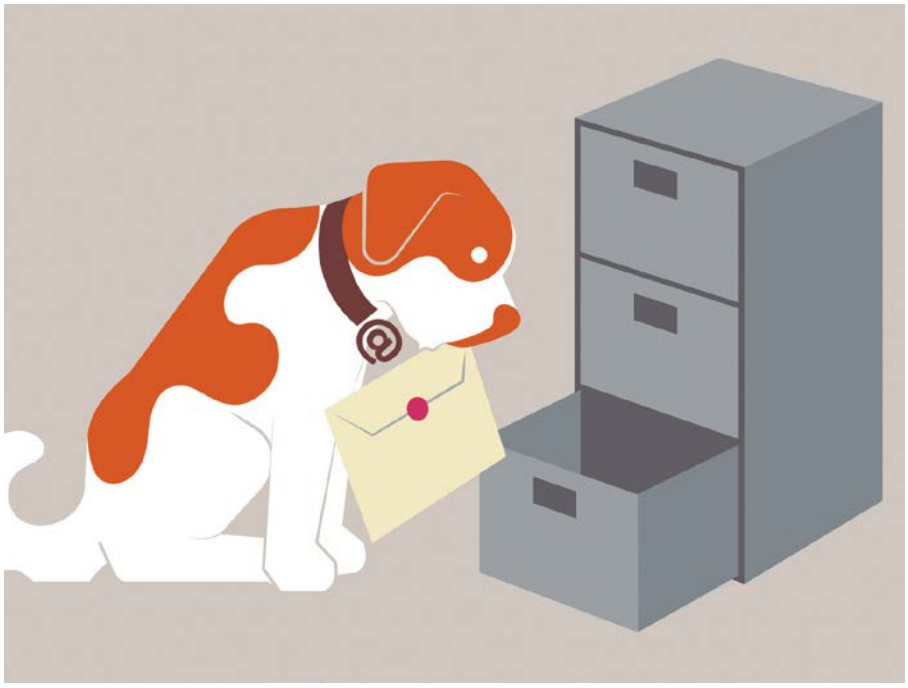
Erklärtes Ziel der SISA ist es, Partnerschaften zwischen der Wirtschaft und den Behörden weiterhin zu fördern und auch künftig gemeinsame, nationale Kampagnen zu führen. Möglichst viele Bürgerinnen und Bürger sollen mit solchen Kampagnen erreicht und sensibilisiert werden, sodass die Schweiz zu einem sichereren Internetland wird.

Werden Sie Mitglied

Die SISA freut sich über neue Mitglieder und Partner. Insbesondere Polizeikorps aus der Schweiz bietet die SISA die Möglichkeit, kostenlos Partner der SISA zu werden. Die Idee hinter einer solchen Partnerschaft ist, dass man sich gegenseitig unterstützt und insbesondere die Produkte der SISA, wie das Präventionsmaterial von ibarry.ch aktiv nutzt und weiterverbreitet. Wir freuen uns, dass bereits diverse Polizeikorps der Schweiz von dieser Möglichkeit Gebrauch machen und damit ihre eigenen Ressourcen schonen. Nehmen Sie Kontakt mit uns auf, am besten auf ibarry.ch (ibarry.ch → Über uns → Kontakt).

iBarry.ch – der orange-weisse Retter wirbt für sicheres Surfen

Er ist herzig, neugierig und tappt jeweils beinahe in die Fallen der Online-Betrüger. So schafft es der Online-Bernhardiner iBarry auf sympathische Art, Aufmerksamkeit auf ein Thema zu lenken, mit dem sich die wenigsten gern auseinandersetzen: den Gefahren im Internet.



zvg

iBarry hat in den vielen Bildern wie hier beim Thema Datensicherung eher menschliche Züge. Zwischendurch benimmt er sich aber auch wie ein Hund und bellt bei Gefahren oder schnuppert neugierig an etwas.

Der Bernhardiner und Lawinensuchhund Barry soll Anfang des 19. Jahrhunderts über 40 Menschenleben gerettet haben. Sein digitaler Nachfolger iBarry will zu Anfang des 21. Jahrhunderts ähnliches fürs Internet schaffen. Dabei hat sich die Rolle des Online-Hundes etwas geändert. Da er die Menschen nicht mehr direkt aufspüren und aus dem Schnee buddeln kann wie sein Vorgänger, geht er stattdessen als

Autorin

Annette Hirschberg
ist seit August 2019 bei der Swiss Internet Security Alliance verantwortlich für Kommunikation und Marketing von iBarry.

zvg

zvg

Beim Thema Smartphone-Sicherheit steigt iBarry kurzerhand ins Handy hinein und schnuppert neugierig an den Icons der Applikationen: Das Herunterladen von Malware ist eine der Gefahren im Umgang mit mobilen Geräten.

zvg

Beim Thema Online-Shopping wird nicht nur beschrieben, wie Betrüger versuchen, ihre Opfer in die Irre zu führen. Anhand eines echten Beispiels wird aufgezeigt, woran man Fake-Shops typischerweise erkennt.

gutes Beispiel voran und erkundet begeistert die Tiefen und Unwegsamkeiten des Internets. Naiv und gutgläubig begegnet er dabei allen möglichen Gefahren, lässt sich von den Betrügern aber nicht erwischen.

Einfache Regeln für eine komplexe Technologie

iBarry verkörpert dabei ein wenig den Durchschnitts-Internetnutzer. Ein Hund, auch ein Rettungshund, verfügt ja über keine besonderen Informatik-Kenntnisse und weiss nicht viel über die Tricks von Betrügern. Dank dieser Charakterisierung und seinem knuddeligen Auftreten kann er vermitteln, dass jedermann Gefahren im Internet erkennen kann. So soll iBarry den sicheren Umgang mit elektronischen Geräten und das sichere Surfen im Netz einfach aussehen lassen.

Das ist bei der Sensibilisierung für Internet-Risiken wichtig: Heute nutzt praktisch die gesamte Bevölkerung vom Kindergartenkind bis zu den Hundertjährigen das Internet, um Nachrichten zu schreiben, Besorgungen zu machen, Informationen abzurufen oder sich zu unterhalten. Gleichzeitig ist die digitale Welt, die dahintersteckt, so komplex und schwierig zu verstehen, dass sich die meisten der Technologie ausgeliefert fühlen. Deshalb zeigt der Bernhardiner auf seiner Plattform für Internetsicherheit der Bevölkerung mit sympathischen Bildern und einfacher Sprache, dass Online-Sicherheit gar nicht so kompliziert ist.

iBarry sensibilisiert mit klaren und einfachen Tipps

Meist gibt iBarry dabei auf seinen jeweiligen Infoseiten zu verschiedenen Themen schon ganz am Anfang ein paar einfache Tipps, wie zum Beispiel beim Thema Sicherheit mobiler Geräte. Hier spricht er seine Leser direkt an und stellt fünf einfache Regeln auf, mit denen jede*r sein Smartphone und das Surfen damit sicherer machen kann:

1 **Handy verriegeln:** Wir nutzen eine starke Zugangssperre zu unserem Smartphone.
2 **Apps überprüfen:** Wir installieren nur Apps aus den autorisierten App-Stores und erteilen nur die nötigsten Berechtigungen.
3 **Updates installieren:** Wir prüfen die Software und Apps auf aktuelle Updates und installieren diese so schnell wie möglich.
4 **Anruf, Nachrichten, Online-Schnäppchen:** Wir lassen uns nicht täuschen und hinterfragen verführerische Angebote.
5 **Öffentliches WLAN mit Vorsicht:** Wir sind uns bewusst, dass alles, was wir im Internet via öffentlichem WLAN tun, von Dritten einsehbar ist.

Für diejenigen, die es genauer wissen wollen, folgen danach die ausführlicheren Texte und Erklärungen, bei denen man weitere Details über ein sicheres Verhalten erfährt.

Zum Teil wird auch mit Hilfe von Screenshots echter Beispiele erklärt, woran man Fake-Shops oder Phishing-Mails erkennt. Das soll Internetnutzern helfen, Kompetenz zu erlangen. Je informierter sie sind, desto geringer ist die Gefahr, dass sie selbst zum Opfer werden.

Spielerisch und mit Hilfe von Tests zu mehr Sicherheit im Netz

Gegliedert ist die Website in die Bereiche «Sichere Geräte», «Sicheres Surfen» und «Risiken im Internet». Dort findet man Infoseiten zu den wichtigsten Themen rund um digitale Sicherheit wie der Umgang mit smarten Geräten (Internet of Things), Datenschutz auf Social Media oder Phishing und Romance Scam.

Nicht nur mit einfach verständlichen Info-Seiten wirbt iBarry für sicheres Verhalten im Netz. Seit Kurzem können Nutzerinnen und Nutzer mit Tests ihre Internetkompetenz spielerisch überprüfen. So erfahren sie beim

Quiz zum Thema Passwortsicherheit, wie gut sie die gängigen Sicherheitsregeln für Passwörter kennen. Weitere Tests folgen in Kürze zu den Themen Smartphone-Sicherheit, Datenschutz, sicheres Surfen und Phishing.

Tests gibt es aber nicht nur, um das Wissen der Nutzerinnen und Nutzer abzufragen, sondern auch für deren Infrastruktur. So stehen mehrere kostenlose Sicherheits-Checks auf iBarry.ch zur Verfügung:

- **Der E-Mail-Check** zeigt an, ob die eigene E-Mail-Adresse bei Datenlecks aufgetaucht ist.
- **Der Netzwerk-Check** überprüft, ob der eigene Computer in den letzten Tagen versucht hat, eine Verbindung zu einem als infiziert bekannten Server aufzubauen.
- **Der Malware-Scanner** sucht den Computer auf Viren, Trojaner und Würmer ab.
- **Der Software-Check** testet, ob auf dem Computer Sicherheitslücken bestehen.

Auch im Bereich Sicherheits-Checks ist zudem geplant, weitere nützliche Testverfahren hinzuzufügen.

Die SISA erarbeitet derzeit auch einen Flyer, der bei Infoveranstaltungen abgegeben werden kann. Dieser kann in Kürze bestellt werden und, wenn gewünscht, zusätzlich mit dem eigenen Logo versehen werden.

Das ehrgeizige Ziel der Swiss Internet Security Alliance (SISA), dem Verein, der iBarry.ch betreibt, ist, die Schweiz mit Hilfe des orange-weissen Bernhardiners zum sichersten Internetland der Welt zu machen. Dazu soll die Plattform für Internetsicherheit zu *der Präventionswebsite für Internetsicherheit der Schweiz* werden. Schon heute verweisen zahlreiche Behörden und Unternehmen auf iBarry.ch. Die SISA freut sich über jedes weitere Engagement, das dieses Ziel unterstützt.

Weitere Informationen unter: ibarry.ch

Weil Cyberkriminalität uns alle angeht

Kaum ein anderer Deliktsbereich stellt die Strafverfolgungsbehörden aktuell vor derart grosse Herausforderungen wie die Cyberkriminalität. Umso bedeutender sind das enge Zusammenspiel von präventiven und repressiven Massnahmen und die Arbeit im Netzwerk. Denn: Für eine effektive Bekämpfung ist eine enge Zusammenarbeit mit diversen Partnern erforderlich.

Vor Cyberkriminalität ist niemand gefeit: Neben Privatpersonen sind immer wieder auch kleinere und grössere Unternehmen, Institutionen oder Verwaltungsbehörden von Cyberattacken jeglicher Art betroffen. Angesichts der zunehmenden Komplexität von Angriffsmethoden und der Professionalisierung der Angreifer wird es immer schwieriger, wirksam gegen Cyberkriminelle vorzugehen oder diese überhaupt zu ermitteln. Nicht zuletzt deswegen und aufgrund der steigenden Fallzahlen kommt der Prävention im Cyberbereich eine grosse Bedeutung zu.

Mit der Sensibilisierungsarbeit zielt die Kantonspolizei Bern darauf ab, auch jene zu erreichen, die sich bislang nicht von dieser Kriminalitätsform betroffen fühlten. Das Internet durchdringt heute nahezu alle Lebensbereiche und wird von den unterschiedlichsten Akteuren genutzt. Ebenso facettenreich sind die Bedrohungen. So kann ein angeblicher Investmentberater («Anlagebetrug») gleichzeitig auch eine betrügerische Liebesbeziehung zu einem Opfer aufbauen («Romance Scam») und damit dieser Person in mehrfacher Hinsicht Schaden zufügen. Ein anderes Beispiel, das die Komplexität der Herausforderungen aufzeigt, sind Unternehmen, die zwar die Mitarbeitenden für Cybergefahren sensibilisieren, dabei aber die notwendigen technischen und organisatorischen Massnahmen vernachlässigen. Ohne die Kombination aller Vorkehrungen werden solche Unternehmen kaum eine Chance gegen organisierte Cyberkriminelle oder technisch versierte Hacker haben.

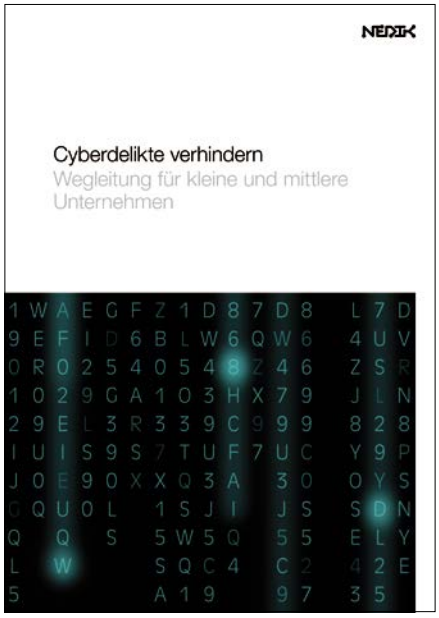
Für die Präventionsarbeit ist es also entscheidend aufzuzeigen, dass bei der Bekämpfung von Cyberkriminalität Themen oder Massnahmen nicht isoliert betrachtet werden dürfen. Vielmehr sind nur eine gesamtheitliche Betrachtungsweise und das Zusammenspiel verschiedener Massnahmen zielführend. Fernziel ist es, dass nicht

Autorin

zvg

Fernanda Gurzeler ist wissenschaftliche Mitarbeiterin Prävention der Fachstelle Projekte und Cyber bei der Kantonspolizei Bern.

zvg



zvg

In Zusammenarbeit mit diversen Partnern entstanden die Broschüren «Wegleitung für Gemeinden» (www.cyber.police.be.ch → Informationen für Gemeinden) und «Wegleitung für KMU» (www.cyber.police.be.ch → Informationen für KMU).

nur die vielen Chancen digitaler Medien, sondern auch die Risiken und die technischen Anforderungen fest im Bewusstsein verankert sind. Dafür ist ein kooperativer Ansatz unerlässlich. Mit Blick auf die verschiedensten Player, Behörden, Unternehmen, Vereine oder Hochschulen, drängt sich eine Zusammenarbeit nicht nur zwischen den Strafverfolgungsbehörden, sondern mit weiteren Partnern auf.

Zusammenarbeit auf nationaler Ebene

Ein Beispiel für dieses Zusammenspiel sind die Informationsunterlagen für KMU und für Gemeinden, die im Rahmen des polizeilichen Netzwerks NEDIK (siehe Kasten), erarbeitet worden sind. Aufgrund der steigenden Fallzahlen und der grossen Schadenssummen haben diverse Schweizer Polizeikorps das Bedürfnis zum Ausdruck gebracht, kleine und mittlere Unternehmen für die Verhinderung von Cyberdelikten zu sensibilisieren. Das Bedürfnis nach mehr Informationen haben auch die kommunalen Verwaltungen geäussert. Ein Ziel aus Sicht der Polizei war es auch, die Geschädigten zu ermutigen, im Falle eines Falles mit den Strafverfolgungsbehörden zusammenzuarbeiten. Denn aufgrund von Untersuchungen muss davon ausgegangen werden, dass viele Betroffene im Schadensfall die Polizei nicht oder erst sehr spät beiziehen.

Koordiniert von der Kantonspolizei Bern und in enger Zusammenarbeit mit dem Nationalen Zentrum für Cybersicherheit (NCSC), der Kantonspolizei Zürich, dem Sicherheitsverbund Schweiz (SVS), dem Bundesamt für wirtschaftliche Landesversorgung (BWL), dem Amt für Informatik und Organisation des Kantons Bern (KAIO) sowie Vertreterinnen und Vertretern der jeweiligen Zielgruppen wurden die Bedürfnisse erhoben und die Situation vor Ort 1:1 erfasst. Dadurch konnten wertvolle Inputs für die Erstellung der Informationsunterlagen gewonnen werden. Denn es ist allen bewusst: Dokumente und Tipps gibt es viele – wichtig ist, dass sie genützt und die Inhalte umgesetzt werden können. Aus diesem Grund stand von Anfang an fest, dass es neben den Dokumenten weitere Instrumente braucht. Bald entstand im Austausch mit weiteren Korps die Idee, Mustervorträge zu diesem Thema zu erarbeiten und eine entsprechende Schulung für Polizistinnen und Polizisten durchzuführen. Weiter arbeitet die Kantonspolizei Bern im Auftrag von NEDIK im Rahmen der Nationalen Cyberstrategie 2018–2022 im nationalen eLearning-Projekt eCyAd mit. Dessen Ziel ist es, die rund 400 000 Verwaltungsmitarbeitenden in der Schweiz zu sensibilisieren.

Die erwähnten Massnahmen finden in Abstimmung mit denjenigen der Schweizerischen Kriminalprävention (SKP) statt und sollen diese ergänzen. Denn neben der Erstellung von Sensibilisierungsmaterialien koordiniert die SKP weitere Massnahmen auf nationa-

NEDIK

Im Auftrag der Konferenz der Kantonalen Polizeikommandanten (KKPKS) haben die Polizeikorps der Schweiz das **Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK)** gegründet. Ziel von NEDIK ist es, die Zusammenarbeit der Schweizer Polizeien im Bereich Cybercrime zu fördern. Im Netzwerk werden die Kapazitäten und Kompetenzen der Kantonspolizeien so weit wie möglich gebündelt und Aktionen sowie Ermittlungen koordiniert, um Cybercrime auch kantonsübergreifend gezielter zu bekämpfen. Durch den Informationsaustausch im Netzwerk werden repressive Massnahmen aufeinander abgestimmt, fachrelevantes Wissen ausgetauscht und Aus- und Weiterbildungsmöglichkeiten angepasst. Im Rahmen von NEDIK geht es ebenfalls um die Förderung und Koordination der Zusammenarbeit im Bereich der Pädokriminalität. Hierbei werden nicht nur das Peer-to-Peer-Monitoring, sondern auch die verdeckten verdachtsunabhängigen Fahndungen im digitalen Raum interkantonal koordiniert.

ler Ebene. Beispielsweise lancierte sie 2019 in Zusammenarbeit mit den Westschweizer Polizeikorps die Kampagne «Und Sie? Hätten Sie ja gesagt?» zu verschiedenen Themen des Cyberbereichs. Dieses Jahr fokussiert die Kampagne auf die Themen Sexting, Anlagebetrug, Immobilienbetrug und Phishing. Zwischen dem 3. und dem 7. Mai steht zudem die Aktionswoche Cybersicherheit an, die innert fünf Tagen der Bevölkerung die wichtigen Schritte zur digitalen Sicherheit näherbringen wird.

Ein Blick in die kantonale Präventionsarbeit

Neben dieser schweizweiten Koordination richtet die Kantonspolizei Bern wie viele andere Korps auch die tägliche Arbeit vermehrt auf Cyber-Herausforderungen aus. Die allermeisten Straftaten im Cybermodus im Kanton Bern gehören zur Kategorie der Wirtschaftskriminalität, darunter Kleinanzeigenbetrug, Phishing, diverse Malware oder Anlagebetrug. Um schnell auf neue Herausforderungen reagieren zu können, gewinnen die präventiven Massnahmen im digitalen Bereich zunehmend an Bedeutung. Dazu gehören Informationen auf der Webseite, Online-Spiele, Webinare oder kurze Erklärfilme, in denen die jeweiligen Betrugsmaschen für die Bevölkerung veranschaulicht werden. Auch hier ist die Zusammenarbeit mit Akteuren aus der Privatwirtschaft, der Verwaltung und dem Bildungsbereich zentral. Sobald wie möglich soll auch der direkte Kontakt zur Bevölkerung wieder gepflegt werden. Hier stehen abgesehen von Messen und Kongressen mit einem breiten Publikum auch Vorträge und Workshops mit spezifischen Zielgruppen – etwa Vertreterinnen und Vertreter von KMU oder Gemeinden – im Vordergrund.

Das Interesse an Vorträgen für Unternehmen und Gemeinden zum Schutz vor Cyberkriminalität ist gross. Dabei ist es wichtig, aktuelle Fallbeispiele aus dem realen Polizeialltag zu integrieren und konkrete Tipps zum Schutz vor diesen kriminellen Handlungen zu geben. Der gegenseitige Austausch nach den Vorträgen ist ein wichtiger Bestandteil dieser Präventionsarbeit, wobei auch die Teilnehmenden gegenseitig voneinander lernen und sich austauschen können.

Kinder und Jugendliche sowie Lehrpersonen sind eine weitere zentrale Zielgruppe der Prävention im Cyberbereich. Zwar ist Medienkompetenz bereits wichtiger Bestandteil des Lehrplans, und einige Organisationen und Unternehmen verfügen über ergänzende Angebote. Insbesondere im Bereich der rechtlichen Rahmenbedingungen oder der Risiken durch aktuelle Phänomene bestehen aber Lücken. Dies wurde zuletzt auch während des Fernunterrichts deutlich, als es zu Vorfällen kam, bei denen ungebetene Gäste den virtuellen Klassenraum störten. Dank rascher Sensibilisierungsmassnahmen konnten über verschiedene Kanäle entsprechende Informationen vermittelt werden.

123RF/Elnur Amikishiyev

Durch Cyberdelikte können hohe Schadenssummen entstehen.

Im Kanton Bern wird das Schulungsangebot zum Thema «Digitale Medien» zudem ab dem Schuljahr 2021/2022 ab der sechsten Klasse flächendeckend angeboten. Neben persönlichen Schulbesuchen sind Ausbildungsprodukte zentral, die ihrerseits mittels digitalen Medien vermittelt werden können: Ein Wissensspiel für Jugendliche zum Thema Sexting und Cybermobbing wurde beispielsweise im Sommer 2020 auf der Website der Kantonspolizei Bern veröffentlicht. Auch bei diesem Projekt wurde im Verbund mit Jugendanwaltschaft, Lehrpersonen und Schulleitungen gearbeitet. Diese Art von Angeboten wird zurzeit – im Austausch mit weiteren Organisationen – ausgearbeitet und aufeinander abgestimmt.

Die bisherigen Erfahrungen zeigen, dass interne und externe Kooperationen bei der Präventionsarbeit, insbesondere auch bei Cyberdelikten, von enormem Nutzen sind, weil unterschiedliche beteiligte Partner bei der Lösungsgestaltung vielfältige Überlegungen und Aspekte einbringen können. Gerade im Rahmen der Zusammenarbeit mit korpsinternen Partnern fliessen wichtige Informationen aus dem Ermittlungsbereich in die Präventionsprojekte ein und tragen so zu einer besseren Qualität der Produkte bei. Im Zentrum aller erarbeiteten Massnahmen geht es letztlich darum, nicht nur so viele Bürgerinnen und Bürger, Schülerinnen und Schüler, Unternehmen und Gemeinden wie möglich zu warnen und für Cyberdelikte zu sensibilisieren, sondern dabei auch fachgerecht das Zusammenspiel der entscheidenden Schutzmassnahmen zu vermitteln.

«Wichtig ist, dass man die Aufmerksamkeit und das Interesse weckt.»

Ein Interview mit der Geschäftsführerin Denise Nick und dem Senior-Berater Manuel Specker von der Agentur Partner & Partner (Winterthur) über Strategie, Schwierigkeiten und Chancen der Präventionskampagne «Digitale Sicherheit»

zvg

Denise Nick

zvg

Manuel Specker

Frau Nick, Herr Specker, Sie sind dabei, eine Kampagne zu realisieren, welche den Bürgerinnen und Bürgern Tipps zur digitalen Sicherheit gibt. Auftraggeber sind die Polizei, der Bund und die Wirtschaft. Sie müssen also ein eher trockenes Thema vermitteln und dabei viele verschiedene Ansprüche berücksichtigen. Was überwiegt: das Entzücken oder das Entsetzen?

Denise Nick (DN): Ganz klar das Entzücken. Es ist ja nicht selten, dass bei einem solchen Setting mehrere Organisationen beteiligt sind. Aber es ist immer wieder spannend zu sehen, wie die Organisationen miteinander funktionieren, wie die Rollenteilung, die Entscheidungswege, die Prozesse sind. Wir finden auch nicht, dass digitale Sicherheit ein trockenes Thema ist. Abstrakt, das ja. Weil man sich damit vielleicht nicht so auskennt. Wir benutzen zwar alle diese Geräte, und im Zeitalter von Homeoffice erst recht. Aber die meisten sind einfach Anwender und nicht so vertraut mit der digitalen Sicherheit.

Manuel Specker (MS): Spannend bei so vielen beteiligten Organisationen ist ja auch, dass man bei einer guten Koordination mit relativ wenig Aufwand auf vielen Kanälen senden kann. Das ist ein riesiges Potenzial, um viele Personen zu erreichen. So einen Verteiler muss man sich sonst mit beachtlichem Aufwand einkaufen.

Gibt es Einschränkungen bei der Realisierung einer Kampagne, wenn die Polizei der Absender ist?

DN: Nein, die digitale Sicherheit ist ja nicht ein typisches Polizeithema. Im Stil und Ton muss sicher eine gewisse Seriosität gewahrt werden, aber das ist nichts Aussergewöhnliches.

Wie gehen Sie an die Umsetzung einer Kampagne heran?

DN: Zuerst wird mal ganz viel gelesen …

MS: Wichtig ist auf jeden Fall, sich am Anfang Gedanken zu machen über die Ziele und die Wirkung, die man erreichen möchte. Das gleicht man mit der aktuellen Situation ab, um abzuschätzen, wie viel bereits bekannt ist. Dann kann man sich an die Grundprinzipien der Kampagne herantasten. Hier geht es darum, wer über welche Kanäle erreicht werden soll und wie diese Kanäle zusammenspielen. Wir fragen uns, wo jemand mit einem Thema in Berührung kommt, wie man weitere Informationen anbieten kann und an welchem Punkt die Handlung ausgelöst wird. Weiter geht es um die Inhalte, die vermittelt werden sollen, und sehr stark auch um die Sprache und die Tonalität. Das ist gerade bei Präventionskampagnen ein wichtiges Thema. Man muss die richtige Mischung finden, um das Ziel zu erreichen. Gemeinsam mit dem Auftraggeber tastet man sich an die Botschaften und deren Visualisierung heran.

DN: Die Recherchephase am Anfang ist bei einem Thema wie Ihrem enorm wichtig. Von verschiedensten Institutionen wurde bereits enorm viel gedacht, geschrieben und publiziert. Da hat es keinen Sinn, die fachlichen Inhalte neu zu erfinden, aber wir mussten erst eine saubere Grundlage schaffen und herausfiltern, was zentral ist.

Wäre es einfacher gewesen, die Inhalte selbst zu erarbeiten?

DN: Nein, es ist eine komfortable Ausgangslage. Da die Inhalte bereits vorliegen, können wir uns voll auf die Vermittlung konzentrieren.

Auf was muss man da achten?

DN: Die Inhalte müssen leicht verständlich sein und das Interesse wecken. Man soll sich mit dem Thema auseinandersetzen und sich dazu informieren, ohne dass es einem zu viel wird und ohne dass man das Gefühl hat, es sei kompliziert und man mache eh alles falsch.

Und wie gehen Sie das an?

MS: Beim Verständnis dafür, dass das Thema wichtig ist, können wir bereits von einem gewissen Grundwissen ausgehen. Viel Aufklärung braucht es hier nicht mehr. Die Herausforderung liegt darin, die Handlungsanweisungen so simpel zu vermitteln, dass man sich die einzelnen Schritte gut merken kann. Dadurch schaffen wir die Zuversicht, dass das Ziel schnell und unkompliziert erreicht werden kann. So steigt die Bereitschaft, das Wissen auch wirklich umzusetzen. Die Leute sollen sich weder bevormundet noch gelangweilt fühlen, sondern lernen, sich selbst zu helfen.

DN: Es ist wie in anderen Präventionsthemen auch. Wir möchten eine Verhaltensänderung bei einem Individuum erreichen. Das ist schön und gut, aber wir müssen auch die Ausgangslage schaffen, damit jemand sein Verhalten wirklich ändern kann. In unserem Setting erreichen wir das über die Landingpage, wo einfach und verständlich beschrieben wird, was man tun muss. Hier kommen Interessierte schnell zu den gewünschten Informationen.

Wie überzeugen Sie die Adressaten vom Nutzen einer Verhaltensänderung?

DN: Mit Alltagsanalogien, also mit Dingen, die man kennt, schaffen wir den Vergleich zum digitalen Raum. Das ist der Kern der Kampagne und der vorliegenden Sujets. Wir zeigen Situationen, in denen man sich üblicherweise schützt und übertragen dieses Verhalten dann auf die digitale Sicherheit, möglichst ohne Zeigefinger, eher mit Humor oder Überraschung.

Welche Rolle spielt denn der Humor in solchen Kampagnen?

MS: Wichtig ist, die Balance zu finden zwischen Ernsthaftigkeit und Humor eines Themas. Nur lustig sein zu wollen, birgt das Risiko, dass man der Ernsthaftigkeit nicht gerecht wird. Das gilt es zu vermeiden. Bei dieser Kampagne geht es um Sicherheit. Da muss man eine gewisse Seriosität ausstrahlen.

Gibt es No-Gos in Präventionskampagnen?

DN: Es gibt Grundregeln. Man weiss inzwischen, dass Drohen relativ wenig bringt. Das Empowerment der Leute funktioniert einfach nicht über Angstmacherei, das sollte man vermeiden.

Kommt es vor, dass Sie eine Umsetzung verwerfen müssen, weil Sie merken, dass es nicht funktioniert?

DN: Das gibt es wahrscheinlich in jedem Prozess, sobald man beginnt, über das «Wie» nachzudenken. Wir definieren jeweils verschieden Routen, verschiedene Realisierungsansätze. Da geschieht es häufig, dass man irgendwo nicht weiterkommt oder dass man realisiert, dass eine der Routen nicht zielführend ist. Manchmal fällt die Wahl am Schluss auf eine Route, von der man gar nicht erwartet hätte, dass sie das Potenzial hat. Es ist einfach ein Weg, den man gehen muss. An diesem Punkt kommen alle Mosaiksteine aus Ausgangslage, Zieldefinition, Briefing, Grafik und Text zusammen, und irgendwann ergibt sich das Bild.

Sie haben uns kürzlich die Kampagnen-Bilder präsentiert, und natürlich gab es Diskussionen, obwohl wir uns bereits für eine Route entschieden hatten. Der Weg zum fertigen Mosaikbild ist offenbar steinig …

DN: Es ist immer spannend zu sehen, was passiert, wenn man mit einem Sujet-Vorschlag kommt. Die einen schauen drauf und sagen: «Jawohl, ich verstehe, um was es geht, das passt.» Andere haben einen eher wissenschaftlichen Ansatz und den Anspruch, dass alles eindeutig und unmissverständlich sein muss. Das ist meist eine Bereicherung, wie in Ihrem Fall auch, weil es zeigt, wie verschieden man ein Bild wahrnehmen kann. Irgendwann kommt aber der Moment, wo man sich entscheiden muss. Irgendwann muss man damit aufhören, alle Meinungen zu berücksichtigen und Kompromisse einzugehen, denn meistens geht dies zulasten der Botschaft. Vor lauter Korrektheit wird das Bild am Ende von der Zielgruppe nicht mehr gut verstanden. Wichtig ist, dass man die Aufmerksamkeit und das Interesse weckt. In der Vertiefung kann dann alles ausführlich und akribisch korrekt sein, aber beim ersten Kontakt muss man auch mal «fünf gerade sein lassen» und auf komplizierte Konstrukte verzichten.

Die Kampagne setzt schwerpunktmässig auf Social-Media-Känale. Passt das zur Polizei?

DN: Die sozialen Medien sind ideal, um den Kontakt zur Bevölkerung herzustellen und näher an die Leute heranzukommen. Wir sehen das hier in Winterthur. Die Stadtpolizei nutzt die sozialen Medien sehr routiniert und hat einen tollen Auftritt auf Tiktok. Das entspricht der neuen Generation. Die Digital Natives lesen kaum Flyer. Viele Themen würden sie gar nicht mitkriegen, aber so wissen sie immer alles. Die Themen werden schnell vermittelt und in kleinen Einheiten. Die Polizei kann sich mit den sozialen Medien ein ganz anderes Image aufbauen. Wenn man nicht von einem Problem betroffen ist, hat man ja wenig Kontakt mit der Polizei. Man merkt gar nicht, dass sie viel umgänglicher und offener ist, als man vielleicht meint.

Auf was sind Sie am meisten gespannt im Hinblick auf die Aktionswoche im Mai?

DN: Was mich extrem interessiert: Sie haben ein riesiges Netzwerk mit sehr vielen Multiplikatoren. Es ist toll, wenn man so viele Kanäle aktivieren kann. Man muss sie aber auch orchestrieren. Damit steht und fällt letztlich die Kampagne. Alle müssen mithelfen und zur richtigen Zeit das Richtige tun. Das bedingt eine gute Organisation und eindeutige Information, so dass für alle glasklar ist, welches Material man wann, wo abholen kann und wie es eingesetzt wird. Das wird sicher eine Challenge, aber das haben wir ja gerne.

Frau Nick, Herr Specker, vielen Dank für das informative Gespräch!

(Das Interview führte Beatrice Kübli)

Neue Kommissionsmitglieder

In den Kommissionen der SKP mussten vier Personen verabschiedet und durften vier neue Mitglieder begrüsst werden.

Fachkommission

Bruno Lüthi, langjähriges und engagiertes Mitglied der SKP-Fachkommission, ausgewiesener Experte im Thema integrale Sicherheit, Verwaltungssicherheit und Einbruchschutz (und vieles mehr!) hat die Fachkommission verlassen, da er in den wohlverdienten Ruhestand tritt. Wir danken Bruno ganz herzlich, dass wir lange Jahre von seinem Fachwissen und seiner Tatkraft profitieren konnten, und wünschen ihm und dem FC Thun alles Gute zur noch engeren gemeinsamen Zukunft!

Für Bruno Lüthi dürfen wir **Markus Friedli** neu in der Fachkommission begrüssen!

Markus Friedli, Fachbereichsleiter Beratung und Projekte der Kapo Bern ist bei Weitem kein Neuling in der Kriminalprävention, sondern engagiert sich seit Jahren im Thema Einbruchschutz und in vielen anderen Bereichen. Wir freuen uns, vom Fachwissen von Markus Friedli in der Fachkommission profitieren zu dürfen!

zvg

Markus Friedli, Fachbereichsleiter Beratung und Projekte der Kapo Bern

Projektkommission

Leider mussten wir auch Kasi Bischoff aus der Projektkommission verabschieden, da er innerhalb der Stadtpolizei Winterthur die Funktion wechseln durfte. Kasi hat über vier Jahre in der Projektkommission die städtischen Korps vertreten, und wir sind dankbar, dass wir mit der Stapo Winterthur und seinem Vertreter Kasi eine sehr innovative und moderne Stadtpolizei in der PK vertreten hatten. Wir danken Kasi Bischoff herzlich für seine stets willkommenen Inputs, seinem konstruktiven Mitwirken und nicht zuletzt für seine stets gute Laune und wünschen ihm alles Gute in seiner neuen Funktion!

Und ebenso herzlich begrüssen wir **Thomas Egloff** als neues Mitglied in der Projektkommission. Er wird ebenfalls die städtischen Polizeikorps vertreten, und wir sind sicher, dass auch er aus der Stapo Winterthur viele nützliche Inputs und Ideen einbringen wird: ein herzliches Willkommen, Herr Egloff!

zvg

Hptm Thomas Egloff, MLaw, Hauptabteilungsleiter

Auch bei unserer Vertretung Ostpol auf Kripoebene mussten wir Roland Hübner der Kapo Appenzell Innerrhoden verabschieden. Roland hat uns viele Jahre begleitet und aus dem kleinen Korps die gesamte Ostschweiz mit Herzblut und viel Initiative vertreten. Wir wünschen Roland auf seinem neuen beruflichen Weg alles Gute und danken ihm für seine stets willkommene Mitarbeit!

Ostpol wird neu über **Stephan Kühne,** Kripochef der Kapo St. Gallen vertreten sein, und wir heissen ihn auch in der Projektkommission willkommen und freuen uns auf die tatkräftige Unterstützung aus dem Osten!

Last but not least hat auch der ehemalige Kripochef der Kapo Schwyz, Stefan Grieder, die Vertretung des Konkordats Zentralschweiz abgegeben, da er im Frühjahr 2021 das Kommando der Kapo Nidwalden übernehmen wird. Wir gratulieren Stefan von Herzen zu seiner neuen Funktion und danken ihm für die langjährige engagierte und konstruktive Mitarbeit in der PK!

zvg

Stephan Kühne, Kripochef der Kapo St. Gallen

zvg

Jürg Wobmann, Kripochef der Kapo Luzern

Als neuen Vertreter der Kripos in der Innerschweiz dürfen wir **Jürg Wobmann,** Kripochef der Kapo Luzern im Kreis der Projektkommission willkommen heissen! Wir freuen uns auf die sicherlich weiterhin engagierte Zusammenarbeit mit den Kapos im Herzen der Schweiz.

Das Paradox der Prävention …

… ist kurz gesagt folgendes: Je besser sie funktioniert, desto mehr könnte man dem Irrtum erliegen, sie sei eigentlich gar nicht vonnöten. Denn der Schaden, den sie verhindern soll, entsteht ja dann tatsächlich nicht, und die Bedrohung ist oft weder sichtbar noch spürbar. Was passieren *könnte,* wenn man ihre Lawinenverbauung *nicht* gebaut hätte, fürchten die Dorfbewohner hingegen auch dann noch, wenn sie hält: Entweder weil sie den letzten Lawinenabgang selbst miterlebt haben oder weil sie die Katastrophenberichte kennen und den schneebedeckten Berg – also die Bedrohung – täglich vor Augen haben. Auch würde wohl niemand, der an einem Sommerabend am See von tausend Stechmücken umschwirrt, jedoch kein einziges Mal gestochen wird, an der Präventivkraft seines Mückensprays zweifeln – zumal wenn er *ohne* ihn noch *jedes* Mal gestochen wurde. Aus Schaden wird man klug; erkannte Bedrohung und Prävention gehören eng zusammen.

Allerdings gibt es da draussen etliche neuartige, nicht so leicht erkennbare Bedrohungen, bei denen der Einzelne nicht auf eigene oder familiäre Erfahrungswerte zurückgreifen kann, z. B. eine Pandemie. Hier muss man für eine effektive Prävention auf Informationen vertrauen, die ausserhalb des eigenen Erfahrungshorizonts liegen. Dabei tritt dann schnell noch ein anderes Präventionsparadox in Erscheinung: Je verletzlicher ich selbst bin, als Angehöriger einer Risikogruppe in der Minderheit, desto mehr profitiere ich von der Präventionsleistung der Allgemeinheit, während die weniger vulnerable Mehrheit nur sehr indirekt und vielleicht langfristig profitiert, aber vor allem unter den Einschränkungen ihres gewohnten Lebensstils leiden muss. Das sind schlechte Nachrichten für die meisten, weshalb viele geneigt sind, die Bedrohung zu verharmlosen oder sogar zu leugnen und die Überbringer der Nachricht für «schuldig» zu halten. Andererseits, wenn's einen dann doch plötzlich schwer erwischen sollte, an wen würde man sich wenden wollen: an «wahrheit24.ch» oder an ein richtiges Krankenhaus?

Bei der Cyberkriminalität, dem Schwerpunkt dieser Ausgabe des SKP INFO, sieht es noch einmal anders aus: Für die meisten Menschen sind die verschiedenen Bedrohungen hier zwar ebenfalls noch eher unbekannt, aber durch schnelle und flächendeckende Aufklärung der Zusammenhänge und breite Schulungsangebote kann die Prävention für alle Beteiligten von Vorteil sein, ohne grösseren Aufwand und ganz ohne Paradox. Natürlich zuerst für jeden Einzelnen, damit er nicht in die Falle tappt und seine Ersparnisse einbüsst, doch auch für die gesamte Wirtschaft drumherum, wenn sie sich einerseits gegen direkte Cyberangriffe wehren und andererseits weiterhin auf die finanzielle Stabilität ihrer ebenfalls wehrhaften Kunden und Partner setzen kann. Was den Einzelnen schützt, schützt hier auch die Allgemeinheit, und umgekehrt.

Noch ein letztes Beispiel für ein Präventionsparadox, Stichwort: Klimawandel. Anders als bei Lawinen, Pandemien und Stechmücken wird es hier vermutlich gar nicht möglich sein, auf sichere Erfahrungswerte zu warten, um nach dem dann erlittenen Schaden effektive Präventionsmassnahmen für die Zukunft entwickeln zu können. Man müsste vielmehr etwas abwenden wollen, das man noch nie gesehen hat. Dafür, dass eine Katastrophe droht, gibt es zwar viele Anhaltspunkte, aber eben keine Beweise; der Mensch müsste wohl erstmals nicht durch *Schaden,* sondern durch *Vernunft* zur Vernunft kommen. Zwar scheint es so, dass auf dem Oberdeck noch gefeiert wird, während der (letzte?) Eisberg den Rumpf des Dampfers bereits aufgeschlitzt hat, aber ob das stimmt, wird man abwarten müssen. Wie hiess noch gleich der berühmte Satz dieser Indianerkönigin? «Erst wenn der letzte Fisch gefangen ist und der letzte Baum sein letztes Blatt verloren hat, erst dann wirst du, weisser Mann, feststellen, dass man das Geld nicht essen kann…», oder so ähnlich. Bis dahin: Maske auf, Virenschutz rein, und wenn das Telefon klingelt, einfach nicht drangehen!

Volker Wienecke
Kontakt: redaktion@skppsc.ch

NEUES AUS DER SKP

«Lass dich nicht sex-erpressen!» Was Sie über Sextortion wissen sollten

Dieser Moment, wenn Menschen realisieren müssen, dass sie mit intimem Bildmaterial erpresst werden, ist für viele schrecklich. So genannte Sextortion-Fälle treten in verschiedenen Formen auf; sei es als Folge eines erotischen Chats oder als Spam. Beide Modi Operandi nutzen den Umstand, dass die Betroffenen vermeiden wollen, dass (vermeintlich) vorhandenes kompromittierendes Bildmaterial öffentlich gemacht wird oder an Freunde und Bekannte geschickt wird, und dafür auch zahlen. Die Präventionsbotschaft ist aber in beiden Fällen eindeutig: *Keep calm and don't pay!*

«Rendite genial? Verlust total!» Was Sie über Online-Anlagebetrug wissen sollten

Immer häufiger werben Betrüger und Betrügerinnen für angeblich vielversprechende neue Anlageformen auf ihren angeblichen Handelsplattformen (Trading-Seiten). Doch wer darauf eingeht und investiert, kann nur verlieren! Der neue SKP-Leporello erklärt verständlich, wie Online-Anlagebetrug typischerweise abläuft, wie Sie sich informieren sollten, bevor Sie z. B. in Kryptowährungen investieren, und was Sie tun sollten, wenn Sie bereits Geld an solche Betrüger verloren haben. Zudem finden Sie allgemeine Tipps, wie Sie schon frühzeitig erkennen können, ob ein Angebot seriös oder höchstwahrscheinlich betrügerisch ist.
Der Leporello ist mit der freundlichen Unterstützung von EBAS («eBanking – aber sicher!») entstanden.

Dein Leben online

Das Leporello im Kreditkartenformat informiert kurz und knapp darüber, wie Jugendliche im Internet miteinander umgehen und wie sie reagieren sollten, wenn sie auf inkorrektes und respektloses Verhalten treffen. Es ist als Ergänzung zu den ausführlicheren «My little Safebook»-Broschüren für Jugendliche und Erziehungsberechtigte gedacht und soll in jugendgerechter Form und Gestaltung die Betroffenen für die entsprechenden Inhalte sensibilisieren.

Alle drei Faltblätter finden Sie unter www.skppsc.ch → Downloads → Broschüren + Faltblätter

DER REIM AUF CRIME

Das oft belastende und traurige Umfeld der Kriminalitätsbekämpfung soll im SKP INFO zukünftig durch einen kleinen humoristischen Beitrag (unserer Leserinnen und Leser!) aufgelockert werden: Das kann ein Gedicht sein, eine Anekdote aus dem Polizeialltag, ein gut erzählter Witz zum Thema oder ein Cartoon. Wer sich angesprochen fühlt und seiner Kreativität freien Lauf lassen möchte, schickt seinen Vorschlag bitte an info@skppsc.ch!

«Cybercrime» von Mario Capitanio, Bern

SKPPSC
Schweizerische Kriminalprävention
Haus der Kantone
Speichergasse 6
Postfach
CH-3001 Bern

www.skppsc.ch