Veranstaltungen

Tipps vom Spezialisten: So vermeide ich Risiken im World Wide Web

Rund 100 Besucher beim Informations- und Austauschabend zum Safer Internet Day

Es gab und gibt sie auch in Ostbelgien: Online-Betrug, gefälschte Rechnungen, Versand von Nacktfotos. Wie man sich schützen kann und wo es Hilfe gibt, war Thema des diesjährigen Informationsabends zum Safer Internet Day.

In diesem Jahr lag der Schwerpunkt auf Fallen, in die ostbelgische Bürger in der Vergangenheit getappt sind. Und davon gibt es einige, wie die Referenten zu berichten wussten:

- Danny Loos von der Föderalen Kriminalpolizei
- Sabine Bierfeld und Marita Brüls vom Büro für Kriminalitätsvorbeugung der Polizeizone Weser-Göhl

Gefälschte Mails / Phishing-Seiten

Ein Betrugsversuch, der auch in Ostbelgien um sich greift: Mails, die aussehen, als kämen sie von einer bestimmten Firma, aber gefälscht sind. Damit soll der Empfänger

veranlasst werden, die vermeintliche Rechnung du
Konto zu begleichen. Hier konnte Danny Loos
einige Bespiele zeigen, die gemeinsam mit
dem Publikum analysiert wurden. Er gab ein
paar konkrete Tipps:

- auf das Aussehen der Mail achten: Oft werden mehrere Schriftarten benutzt, was seriöse Firmen selten tun.
- auf die Mailadresse achten: Eine Adresse mit „….@cannabis.org" sieht nicht nach einem seriösen Anbieter aus.
- Häufig sind Sprachfehler vorhanden und /oder der Adressat wird geduzt.
- Die Mail fordert dazu auf, auf einen Link zu klicken und auf der erreichten Webseite ein Formular auszufüllen. Hier sollte man die Endung der Webadresse prüfen: Wenn die Webseite mit Hilfe eines Gratis-Webseitenprogramms erstellt worden ist, sind Zweifel angebracht.
- Führt der Link auf eine Zip-Datei (die Dateiendung wird sichtbar, wenn der Mauszeiger darauf steht), diese auf keinen Fall öffnen. Sie enthält vermutlich Schadsoftware.
- Falls die Mitteilung in der Mail z.B. lautet, die Kontonummer der Firma habe sich geändert und der Kunde möchte bitte auf das neue Konto überweisen: die IBAN-Nummer kritisch prüfen. Ist das plausibel? Im Zweifelsfall bei der Firma nachfragen.

Dubiose Online-Shops

Gefälschte Online-Shops kassieren Geld, liefern aber die Ware nicht. Hier geht es entweder um Betrug oder um Datenklau. Auch hier hatte Danny Loos einige Tipps:

- auf der Webseite im Impressum nachsehen. Seriöse Anbieter veröffentlichen dort Namen, Postanschrift und Telefon-Kontaktdaten.
- auf das Schloss-Symbol und die Adresse im Browserfenster achten: Steht weder Schloss noch „https" vor der eingegebenen URL, ist Vorsicht bei der Eingabe von persönlichen Daten geboten: Diese Verbindung ist nicht gesichert.

- Was zu gut ist, um echt zu sein, ist es meistens auch nicht: Werden Markenartikel zu sehr günstigen Preisen angeboten, ist Misstrauen angesagt.
- Im Zweifel überprüfen, wer der Inhaber der Domain ist. Ist die Seite eines vermeintlich deutschen Shops z.B. auf einen Anbieter in China registriert, kann etwas nicht stimmen.
- Auf Gütesiegel wie „certified shop" achten.

Romantik-Betrug

Gesundes Misstrauen ist auch angesagt, wenn Singles z.B. über ein Dating-Portal oder Facebook kontaktiert werden: Dahinter kann ein Romantik-Betrug lauern. Hier geht es um das Anbahnen einer Online-Beziehung, mit dem Ziel, Geld zu erbeuten.

Häufig geben sich Männer als amerikanische Soldaten oder Ingenieure aus, Frauen als Krankenschwestern oder Ärztinnen. In jedem Fall aber wird suggeriert, dass der Betreffende gerade in einem fremden Land festsitzt und Geld braucht.

Dass diese Betrugsmasche häufig vorkommt, konnten zwei Bankangestellte aus dem Publikum bestätigen: Sie haben ermittelt, dass auf diese Weise in den letzten Jahren bis zu einer halben Million Euro von Ostbelgiern gezahlt worden sind!

Sexting

Um Beziehungen anderer Art ging es im Beitrag von Sabine Bierfeld und Marita Brüls vom Büro für Kriminalitätsvorbeugung der Polizeizone Weser-Göhl: den Versand von Nacktfotos, auch „Sexting" genannt.

Besonders häufig tun dies Jugendliche im ersten Überschwang des Verliebtseins. Ist die Beziehung dann zu Ende, werden die freizügigen Fotos dann aus Rache an andere weitergeleitet.

Die beiden Polizistinnen erklärten ausführlich, was dahinter steckt, wie die Rechtslage aussieht und wie Eltern dem vorbeugen können. Besonders brisant: Die Jugendlichen sind sich meist der Tatsache nicht bewusst, dass sie sich strafbar machen.

Freizügige Fotos von Minderjährigen fallen in die Rubrik „kinderpornografisches Material", selbst wenn sie ursprünglich mit Einverständnis der Abgebildeten gemacht wurden. Hier drohen empfindliche Strafen: In der Regel wird das Material beschlagnahmt (damit sind Handy und/oder der Computer weg), Eltern haften für ihre Kinder und müssen die Kosten die Entschädigung des Opfers erstatten.

Datenlecks

Zum Abschluss ging es noch um gehackte Mailkonten, schlechte Passwörter oder den leichtsinnigen Umgang der Nutzer damit. Auch hier hatten die Experten zahlreiche

interessante Tipps für die Zuhörer, wie sie sichere Passwörter erstellen und sie ebenso sicher aufbewahren können

Die Liste der genannten hilfreichen Webseiten und Anlaufstellen haben wir für Sie im Download bereitgestellt.

2004 erklärte die Europäische Kommission den 2. Dienstag im Februar zum Tag des sicheren Internets, um auf Risiken und Gefahren aufmerksam zu machen. Mittlerweile beteiligen sich 110 Länder weltweit daran. Zum „Safer Internet Day 2019 " hatten BRF und Medienzentrum Spezialisten der Polizei eingeladen, die darlegten, welche Betrugsversuche in Ostbelgien in der Vergangenheit gemeldet wurden. Der Abend fand mit Unterstützung des Informationsbüros „Europe direct" statt.

Ansprechpartner

Medienzentrum

Gaby Zeimers

Bereichsleiterin
Hookstraße 64
4700 Eupen
Belgien
Tel.: +32 (0)87 555 551
gaby.zeimers@dgov.be
Webseite

Downloads

Handzettel „Internetseiten".pdf [0,16 MB]

Handzettel „Anlaufstellen".pdf [0,14 MB]