Freitag, 05.06.2015, 15:39 Uhr

"Wir sind selbst die Schwachstelle, wenn wir leichtfertig und sorglos im Netz unterwegs sind"

Der Kriminologe Markus Wortmann rät zu einem vorsichtigen Verhalten im Web

SICHERES NETZ HILFT e.V.

Internet, Handy und Co. bringen viele Vorteile mit sich: Schnelle Informationsbeschaffung, kurze Wege, Unterhaltung, Vernetzung. Doch die digitale Welt birgt auch Gefahren. Schadprogramme, Phishing, Mobbing, Hackerangriffe - die Möglichkeiten, das Netz zu missbrauchen, sind ebenso grenzenlos wie es das World Wide Web ist. Der Schlüssel zu mehr Sicherheit liegt im persönlichen Know-how. Je aufgeklärter und kompetenter Anwender sind, desto besser können sie Risiken einschätzen und minimieren. Neben technischen Lösungen geht es hier vor allem um das eigene Verhalten, also den Umgang mit den digitalen Medien.

Kriminologe Markus Wortmann gründete den Verein "Sicheres Netz hilft". Mit ihm sprach Beatrix Gutmann, Leiterin Community und Social Media der Westdeutschen Verlags- und Werbegesellschaft (WVW) und der Ostruhr-Anzeigenblattgesellschaft (ORA) über Chancen und Risken der "neuen" Medien gesprochen.

Schwachstelle Nensch

Der Verein beschäftigt sich mit organisierter Kriminalität, Internet-Kriminalität,

Vorratsdatenspeicherung, Cybermobbing und der Bekämpfung von Kinderpornographie. Wo lauert die größte Gefahr?

Markus Wortmann: Ich möchte an dieser Stelle gerne ein Zitat von Jacques-Yves Cousteau verwenden: "Das Übel kommt nicht von der Technik, sondern von denen, die sie missbrauchen." Schwachstelle Mensch: Auf der einen Seite haben wir es mit Tätern zutun, die sowohl als Einzeltäter, aber insbesondere auch im organisierten Bereich professionelle ‚Schwachstellenanalyse' betreiben - mit dem Ziel, anderen Menschen bewusst und gewollt finanziell zu schaden und / oder einen Imageschaden hervorzurufen.

Häufig werden Daten von Unternehmen und Firmen unter Verwendung von Hard- und Software (sog. Trojanern etc.) ausgespäht und seitens der Cybercriminellen verwendet und / oder im Netz angeboten und mit enormen Gewinnmarchen veräußert. Die Täter agieren überwiegend aus dem Ausland heraus, um unentdeckt agieren zu können. Ihnen hilft die Tatsache, dass aufgrund rechtlicher Hindernisse (unterschiedliche Rechtslagen, Rechtshilfeersuchen etc.) Täterermittlungen häufig ins Leere laufen. Die Gründe hierfür sind vielschichtig.

Die Anzeigebereitschaft von gefährdeten und betroffenen Unternehmen ist optimierungsbedürftig. Der zu erwartende Imageschaden schreckt viele Unternehmen ab, Strafanzeige zu erstatten. Konsequenz: Ein großes Dunkelfeld. Wer möchte schon gerne über sein Unternehmen erzählen, dass es „gehackt" worden ist und Kundendaten abhanden gekommen sind?

Wir müssen uns bewusst machen, dass die Gefahr nicht immer aus fernen Ländern droht, sondern wir selbst die Schwachstelle darstellen, wenn wir leichtfertig und sorglos im Netz unterwegs sind, Daten von uns preisgeben oder die einfachsten Sicherheitsstandards nicht verinnerlicht haben.

Geheimdienste, Institutionen, Anbieter, Gewerbetreibende etc. können doch nur mit Daten arbeiten, die wir ihnen tagtäglich freiwillig zur Verfügung stellen. Die Gefahr sitzt in den meisten Fällen vor dem Personalcomputer und / oder an mobilen Endgeräten. Auch wenn unsere Kinder und Jugendlichen mit diesen Medien aufgewachsen sind und

diese mittlerweile einen hohen Stellenwert genießen, gibt es eine Vielzahl von Menschen, die lediglich Anwender sind. Hier sehe ich eindeutigen Optimierungsbedarf, indem Menschen über den Nutzen, aber auch über mögliche Gefahren aufgeklärt und sensibilisiert werden. Die Vermittlung von Internetsicherheit und die Erlangung von Medienkompetenz stellt eine gesamtgesellschaftliche Aufgabe dar.

Vorsicht ist der beste Schutz

Was kann ich als normaler Nutzer tun, um meine Daten möglichst sicher zu machen. Gibt es eine Handlungsempfehlung?

Markus Wortmann: Die wichtigsten Tipps für deutlich mehr IT-Sicherheit sind:

- Verbinden Sie Ihren Computer niemals ohne Firewall mit dem Internet!
- Surfen Sie niemals als administrativer Benutzer im Internet, sondern nur mit eingeschränkten Rechten!
- Geben Sie niemals vertrauliche Daten weiter (z.B. Passwörter, PIN, TAN, Konto- und Kredikartendaten, Zugangsdaten, Accounts etc.)!
- Keine Zugänge ohne Passwort!
- Wahl eines sicheren Passwortes!
- Keine Passwörter im Browser speichern!
- Verwenden Sie immer eine aktuelle Antivirus-Software auf ihrem Computer, aber auch auf mobilen Endgeräten!
- Setzen Sie nur aktuelle Software auf Ihrem PC, Smartphone, Laptop etc. ein!
- Installieren Sie niemals Software fragwürdiger Herkunft!
- Führen Sie kontinuierlich eine Datensicherung durch!
- Sperrung kostenpflichtiger Rufnummern und Einrichtung der Drittanbietersperre!
- Erst denken, dann klicken!
- Vorsicht ist der beste Schutz!

Eine Sprache für alle

Die Europäische Union will den Datenschutz reformieren. In Zukunft soll nur noch eine Verordnung als Datenschutzgesetz für alle 28 Mitgliedsstaaten gelten. Ist das

sinnvoll?

Markus Wortmann: Bedenkt man, dass der Grundstein des Internets 1969 gelegt wurde und wir mittlerweile weltweit 2,9 Milliarden Internetnutzer haben (davon alleine in der Bundesrepublik Deutschland 58,6 Millionen), freue ich mich sehr über die Bestrebungen. Dass zukünftig alle 28 Mitgliedstaaten nur noch eine Verordnung zum Datenschutzgesetz haben sollen, ist lobenswert. Das Internet ist ein Informations- und Kommunikationsmedium, hier sollten alle Beteiligten eine Sprache sprechen.

Manchmal ist weniger mehr

Wie kann ich mich vor Datenklau schützen?

Markus Wortmann: Sich Medienkompetenz aneignen! Zzudem sollte sich jeder einmal fragen, was einem die eigene Sicherheit im Netz wert ist. Erst denken, dann klicken! Vorsicht ist der beste Schutz! Ganz einfach: Manchmal ist weniger mehr.

100 Prozent Schutz gibt es nicht

Es gibt immer wieder Warnungen im Netz, dass Trojaner eingeschleust werden, Falschmeldungen im Umlauf sind, oder Phishing-Mails Bankdaten abgreifen möchten. Wie kann ich dem Internet überhaupt trauen?

Markus Wortmann: Vorab muss man wissen, dass es einen hundertprozentigen Schutz im Netz nicht geben kann und wird. Durch die Verwendung von geeigneten Sicherheitsprogrammen und der Überprüfung der Sicherheitseinstellungen, aber auch durch seriöses Anwenderverhalten, lassen sich Schäden im Vorfeld minimieren. Leider gibt es immer noch Anwender, die nicht regelmäßig Sicherheitsupdates durchführen, sichere Passwörter verwenden oder neue Betriebssysteme nutzen. Aus Neugier wird eine Mail mit einem Gewinnversprechen geöffnet (Anhang Datei, Verlinkung, Kontaktfeld etc.), die eine Schadsoftware beinhalten kann. Wichtig ist: Erst denken, dann klicken! Meist kann man den Übeltäter anhand der Kopfzeile und an der Rechtschreibung erkennen. Zudem ist zu erwähnen, dass keine seriöse Bank Kunden nach der PIN oder einer TAN fragen würde. Wer heute noch eine Überweisung ohne einen TAN-Generator oder über das Mobile TAN-Verfahren durchführt, handelt fahrlässig und riskiert zudem, Opfer einer Straftat zu werden.

Straftaten anzeigen!

An wen kann ich mich wenden, wenn ich Opfer von Internetbetrug, Cybermobbing oder Stalking geworden bin?

Markus Wortmann: Ganz wichtig ist: Ruhe bewahren! Zudem sollten Sie einem Menschen ihres Vertrauens davon erzählen. Darüber hinaus ist wichtig, dass Sie alle Informationen auf beweiserheblicher Grundlage dokumentieren und archivieren. Es handelt sich hierbei nicht um Kavaliersdelikte. Der Sachverhalt sollte zur Strafanzeige gebracht werden. Jede Polizeidienststelle wäre hier als Ansprechpartner zu benennen. Im Bedarfsfall sollte über die Beauftragung eines Fachanwaltes sowie die Hinzuziehung einer Opferorganisation nachgedacht werden. Es geht nicht um die Bestrafung des Täters, sondern um die Tatsache, dass dem Opfer in seiner physischen und psychischen Notlage zeitnah geholfen wird.

Meist im nahen Umfeld

Wie sieht ein klassischer Fall von Cybermobbing aus?

Markus Wortmann: Leider kommt es immer wieder vor, dass Kinder und Jugendliche in ‚ungünstigen' Situationen (z.B. Toilette) von Dritten fotografiert werden. Zudem finden sich im Datennetz Fotos und Videos in denen Personen ‚freizügig' ins Netz wie z.B. YouNow, Youtube, Facebook, WhattsApp vetc. posten. Schnell machen diese Bilder und Videos in dem Netzwerk ihre Runde.

Die Folge: Die Betroffenen werden mit der Sichtbarkeit und Darstellung konfrontiert, gehänselt, gemieden, beleidigt, bedroht und und und. Meist findest das im unmittelbaren Nahbereich (Freundeskreis, Schule) statt.

Der physische und psychische Druck stellt für die Betroffenen einen erheblichen Leidensweg dar, der sich in Essstörungen, Magersucht, Ängsten, Schlafstörungen, Leistungsschwäche, Konzentrationsschwierigkeiten, Fernbleiben von der Schule bis hin zum Suizid äußern kann.

Ansprechbarkeit, Sensibilisierung, Aufklärung, Begleitung stellen hier auf allen Ebenen der Erziehungsinstanzen (Elternhaus, Schule, Beruf) die Grundvoraussetzung dar. Die Einschaltung von Ermittlungsbehörden und Opferschutzorganisationen ist zu

berücksichtigen.

Bei dem Phänomen Cybermobbing handelt es sich nicht um ein „Kavaliersdelikt“ sondern um verschiedene Einzeldelikte wie Verletzung von Persönlichkeitsrechten, Urheberrechtsverstöße, Bedrohung, Beleidigung etc., die eine Straftat darstellen und zur Strafanzeige gebracht werden sollten. Hier sind wahrlich die Erziehungsinstanzen gefordert.

Stadtteil: München
Erscheinung: Woche 24 - 2015
Autor: job
Serie: Das geht uns alles an
Druckansicht