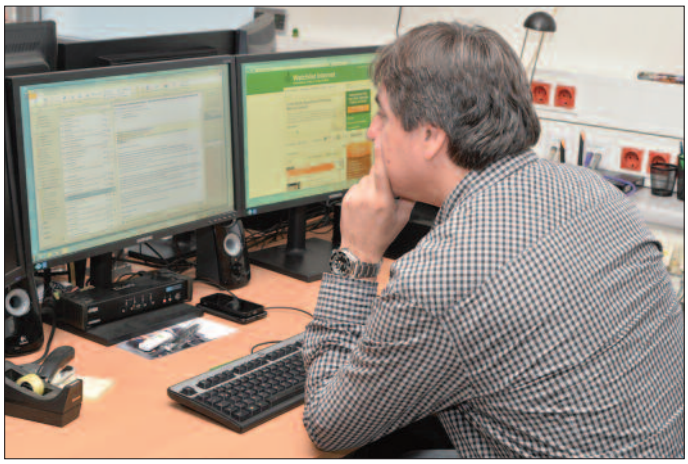
Sensibilisieren und informieren

In der Cybercrime-Meldestelle des Bundeskriminalamts langen jährlich etwa 12.000 Hinweise ein. Die meisten Fälle betreffen Betrug, Erpressung und Datendiebstahl über das Internet.

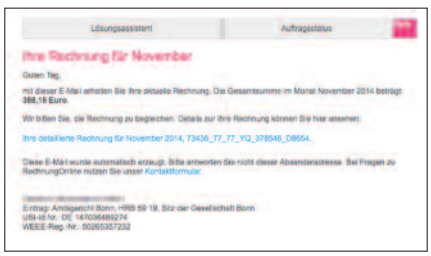
Die meisten der bei uns einlaufenden Hinweise betreffen nicht Cybercrime-Delikte, sondern Betrugsdelikte über das Internet“, sagt Chefinspektor Manfred Meikl, Leiter der C4-Meldestelle beim *Cybercrime-Competence-Center (C4)* des Bundeskriminalamts. „Oft sind es auch straflose Vorbereitungshandlungen zu einem Betrugsversuch“, erklärt der Kriminalbeamte. Dazu zählen vor allem E-Mails von Betrügern, in denen sie ihren potenziellen Opfern hohe Gewinne oder Provisionen versprechen, wenn sie ihnen helfen, ein angeblich großes Vermögen aus einem Land in ein anderes zu transferieren. Um an das Geld heranzukommen, müssen Vorausgebühren oder Bestechungsgelder bezahlt werden, an denen sich das Opfer beteiligen muss. Ein Niederösterreicher zahlte 10.000 Euro, um an seinen vermeintlichen Gewinn von 800.000 Euro bei der angeblichen „Spanischen Lotterie“ zu gelangen. „Der Mann hat sich vorher noch bei uns erkundigt, ob er das Geld überweisen soll, obwohl er gar nicht mitgespielt hat“, schildert Meikl. „Wir haben ihm vergeblich davon abgeraten.“



Cybercrime-Meldestelle des Bundeskriminalamts: Die Mitarbeiter bearbeiten jährlich rund 12.000 E-Mail-Anfragen.

Geld und Daten. Manche Betrugsarten kommen in Wellen. In den meisten Fällen geht es um das Abschöpfen von persönlichen Daten und um Abzocke. Einmal sind es die „Polizeitrojaner“, die den Computerbildschirm sperren und für dessen Freigabe „Lösegeld“ verlangt wird. Dann sind es gefakte E-Mail-Mitteilungen eines Telekom-Anbieters, einer Bank oder des Paketzustellers *DHL*. Wer die Links in solchen Nachrichten anklickt, lädt unbemerkt Schadsoftware auf seinen Computer oder kommt auf eine Seite, auf der er seine persönlichen Daten eingeben soll. Beim Anklicken des Links in der angeblichen *DHL*-Mail lädt er den Lösegeld-Trojaner „Cryptolocker“ auf den Rechner, der Dateien auf den Computern der Opfer verschlüsselt und unbrauchbar macht. Die Täter verlangen für die Entschlüsselung eine „Gebühr“. „Wer das Geld, etwa 500 US-Dollar, innerhalb einer bestimmten Frist nicht bezahlt, dem wird als Strafe das Doppelte vorgeschrieben“, erklärt Manfred Meikl. Die Täter verlangen, dass die „Gebühr“ in der virtuellen Währung *Bitcoin* bezahlt wird.

Auch betrügerische Anrufe von angeblichen *Microsoft*-Mitarbeitern kommen immer wieder vor. Sie sagen Benutzern von Computern mit *Windows*-Betriebssystemen, ihr PC sei mit einer Schadsoftware befallen und bieten ihnen gegen Bezahlung die Reparatur und eine Fernwartung des PCs an. Dazu soll ein Remote-Programm von einer Internetseite heruntergeladen und auf dem Rechner installiert werden. Hat der Täter dann Zugriff auf das System, werden die persönlichen Daten wie E-Mail-Adressen, Passwörter und Bankdaten ausgespäht. Eine andere Masche ist es, E-Mails zu verschicken, in denen um finanzielle Hilfe ersucht wird. Betrüger verschicken mit gehackten E-Mail-Accounts automatisiert Nachrichten an den Verteiler des Betreffenden und bitten die Empfänger um finanzielle Hilfe, da ihnen im Urlaub die Brieftasche und Dokumente gestohlen worden seien. Das Geld soll ihnen über einen Bargeldtransferdienst überwiesen werden.


Lösungsassistent Auftragsstatus

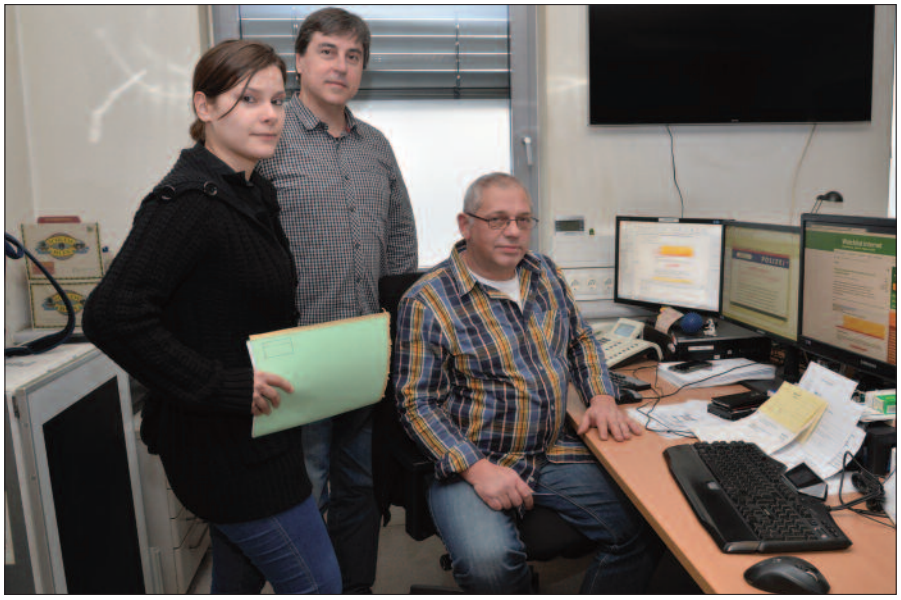
Ihre Rechnung für November

Gefakte Mitteilung eines Telekomanbieters: Link lädt Schadsoftware auf PC.

Immer wieder langen Fälle von „Love-Scams“ in der Meldestelle ein. Betrüger machen sich an ihre potenziellen Opfer in Chat-Foren heran, auf Online-Partnerbörsen oder in sozialen Netzwerken. Sie heucheln Romantik und Liebe vor, um an ihr Ziel zu gelangen: Geld. „Meist sind es Frauen, die sich bei uns melden. Sie können es nicht fassen, dass sie einem Betrüger aufgesessen sind“, berichtet Meikl. „Da bedarf es eines besonders sensiblen Umgangs mit den Geschädigten, um ihnen die Situation zu erklären. Dies trifft auch in Fällen der *Skype*-Erpressung zu. Dabei wird das Opfer über soziale Plattformen zu einem Video-Chat via *Skype* eingeladen. Beim Chat werden die fast ausschließlich männlichen Opfer dazu verführt, intime Handlungen an sich vorzunehmen. „In weiterer Folge wird das Opfer mit der Drohung der Veröffentlichung der heimlich gefilmten Aufnahmen auf einer sozialen Plattform erpresst“, berichtet Meikl.

Gier und Leichtsinn. „Bei allen Geschäften und Angeboten über das Internet ist der Hausverstand einzusetzen“, sagt Cybercrime-Experte Meikl. „Oft sind Dinge oder Versprechen, die über das Internet angeboten werden, einfach zu schön, um wahr zu sein.“ Dennoch fallen viele auf plumpe und fadenscheinige Angebote herein. „Wer sich von einem vermeintlich finanziellen Angebot locken lässt, dem kann man nicht helfen“, sagt Meikl. Die Menschen handeln meist aus Gier, Verblendung oder Leichtsinn. „Viele Betroffene melden sich bei uns, wenn sie ein

FOTOS: ARCHIV, EGON WEISSHEIMER



Cybercrime-Meldestelle des Bundeskriminalamts: Julia Pelikan, Thomas Höchsmann, Manfred Meikl.

verlockendes Angebot auf schnelles Geld per E-Mail bekommen, und fragen, was sie tun sollen, obwohl ihnen selbst bereits klar ist, dass es sich nur um einen Schwindel handeln kann. Oder es sind Opfer, die auf dubiose Angebote hereingefallen sind und uns dies dann mitteilen", berichtet Meikl. Das Geld ist in solchen Fällen weg, denn die Betrüger sitzen meist im Ausland und die Transaktionen finden fast ausschließlich über Bargeldtransferdienste statt, da hier eine Rückverfolgung schwierig und eine Überwachung der Auszahlung nahezu unmöglich ist.

Tipps gegen Betrüger. Die Cybercrime-Experten der Meldestelle raten Betroffenen, die eine offensichtlich betrügerische E-Mail erhalten haben, auf keinen Fall zu antworten. Unter keinen Umständen sollte man angehängte Dateien von unbekannten Absendern öffnen oder in solchen Mails angeführten Web-Links folgen. „In den meisten Fällen raten wir, die Mail sofort zu löschen, vor allem dann, wenn jemand die gleiche Mail schon zigmal erhalten hat", rät Meikl. Wichtig ist, dass Nutzer ihre Antiviren-Programme aktuell halten und die in den meisten Betriebssystemen integrierte Firewall aktiviert haben. „Auf Grund unserer Erfahrungen, können wir schnell und effizient helfen. Wir orientieren uns zudem an Internet-Beobachtungsportalen wie *mimikama.at* und *watchlist-internet.at* sowie an anderen Online-Portalen", sagt der Meldestellen-Leiter.

Die Mitarbeiter der Meldestelle nehmen außer in dringenden Fällen keine Anzeigen entgegen. „Wir verweisen an die örtlich oder fachlich zuständigen Polizeidienststellen", sagt der Meldestellenleiter, der in seiner Arbeit von einer Kollegin und zwei Kollegen unterstützt wird – alle Polizisten und Cybercrime-Experten. „Im Anlassfall erledigen wir für die nachgeordneten Dienststellen auch Erhebungen im Internet. Etwa, wenn Gewaltvideos auf sozialen Plattformen oder anderen Onlinediensten angezeigt werden, oder wenn jemand im Netz seinen Selbstmord ankündigt. „In solchen Fällen versuchen wir die betroffene Person so rasch wie möglich auszuforschen und sie durch Einsatzkräfte zu kontaktieren, bevor es tatsächlich zu einer Tragödie kommt. Die Erfolgsquote ist dabei relativ hoch, wobei es sich bei den Kontaktierten oftmals um vereinsamte Menschen mit Problemen oder einfach um Scherzbolde handelt", betont Meikl.

Wenn neue Betrugsvarianten auftauchen, melden das die Meldestellen-Mitarbeiter intern und der Pressestelle des Bundeskriminalamts. Von dort werden Warnhinweise an die Öffentlichkeit weitergegeben.

Nach missverständlicher Informationen in der Öffentlichkeit meldeten Empfänger von Spam- und Phishing-Mails diese eine Zeit lang an die C4-Meldestelle weiter. „Das hat uns in unserer Arbeit gelähmt", sagt Meikl. „Die Zurückverfolgbarkeit dieser Mails ist nahezu unmöglich und würde auch nicht den Aufwand dafür rechtfertigen." Eine Rückverfolgung und Ermittlung der Urheber bei Massen-Mails ist nur im Anlassfall und nur mit internationaler Zusammenarbeit möglich.

Rund 12.000 E-Mail-Anfragen langen jährlich in der Cybercrime-Meldestelle *(against-cybercrime@bmi.gv.at)* ein, wovon ein Großteil beantwortet wird. „Wir bearbeiten außerdem pro Tag im Schnitt 30 telefonische Anfragen, sind Ansprechpartner für die Wirtschaft sowie die nationalen und internationalen Polizeibehörden und vermutlich die Einzigen, die bei einem stundenweisen Ausfall des Internets nicht darüber klagen würden", sagt Meikl ironisch. Die Meldestelle ist für dringende Fälle rund um die Uhr mit einem Journaldienst besetzt, der im Anlassfall direkt auf weitere Spezialisten des C4 zurückgreifen kann. Organisatorisch untersteht sie dem Leiter des *Cybercrime-Competence-Centers*.

Kontakt: BK 5.2 – C4-Meldestelle, Bundeskriminalamt, 1090 Wien, Josef-Holaubek-Platz 1, against-cybercrime@bmi.gv.at, +43-1-24836-986500.

FOTO: EGON WEISSHEIMER

C4-MELDESTELLE

Aufgaben

- Zentralstelle zur Entgegennahme von Cybercrime-Verdachtsfällen.
- Ansprechpartner und Schnittstelle zu Journaldiensten anderer BMI-Dienststellen und den Landeskriminalämtern.
- Internationaler Ansprechpartner und Schnittstelle zu Europol, Interpol sowie den Kontaktstellen des G8-24/7-Netzwerks (Informations-Netzwerk der G8-Staaten zum Nachrichten- und Informationsaustausch).
- Schnittstelle unter anderem zu CERT-Österreich und zur Wirtschaftskammer (WKÖ).
- Interne Schnittstelle zu den Fachreferaten.
- Telefonische Unterstützung bei IT-Delikten.
- Veranlassung, Koordinierung und Erledigung von operativen Maßnahmen.