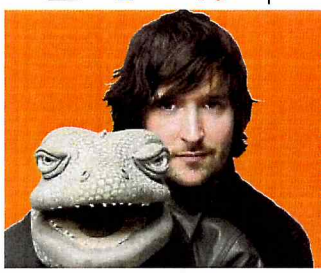
Freitag	Samstag	Sonntag
min 2° max 18°	min 6° max 19°	min 5° max 17°



DIE ECHSE „ECHSOTERIK"

Michael Hatzius

Der preisgekrönte Puppenspieler und Comedian kommt mit seiner neuen Soloshow „Echsoterik" nach Allensbach. Am Donnerstag, 21. März, 20 Uhr, im Pfarrheim Allensbach. Mehr Freizeit-Tipps auf

Seite 17

Die grüne Infrarot Heizung
redwell INFRAROT HEIZUNGEN
Ökologisch und ökonomisch immer auf der richtigen Seite!
Redwell Store Bodensee
Wollmatinger Str. 1, 78467 Konstanz
info@redwell-bodensee.de
www.redwell-bodensee.de

Im Anzeiger-Gespräch: Professor Jürgen Neuschwander, Dekan der Informatik-Fakultät der HTWG

„Die **Angriffe** auf Smartphones nehmen stark zu"

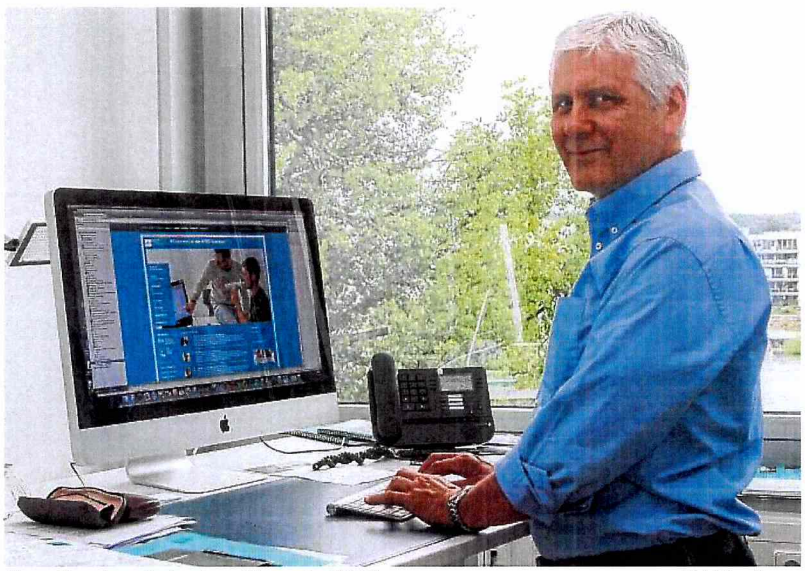
Die Cyberkriminalität ist für Privatpersonen wie für Unternehmen und Staaten eine ernst zu nehmende Gefahr geworden. Wir sprachen mit Professor Jürgen Neuschwander darüber, ob man überhaupt noch mit Kreditkarte zahlen sollte, über gezielte Angriffe von Hackern und über das Verfolgen digitaler Spuren.

Herr Neuschwander, was versteht man eigentlich unter Cyberkriminalität?
Cyberkriminalität umfasst die Straftaten, die sich gegen IT-Systeme oder deren Daten, Datennetze oder das Internet richten, oder die mit Hilfe von IT-Systemen begangen werden. Dabei unterscheidet man noch die Cyberspionage, die sich z. B. auf Computersysteme von Organisationen oder Firmen richtet, mit dem hauptsächlichen Ziel, Know-how abzuziehen. Man geht für 2018 von ca. 50 Milliarden Euro Schäden durch Cyberkriminalität aus.

Können Sie Beispiele für große Angriffe nennen?
Die Trends sind neben Phishing vor allem Verschlüsselungstrojaner, die die IT-Systeme von Organisationen oder Firmen befallen und die Daten auf der Festplatte verschlüsseln, so dass diese nicht mehr nutzbar sind. Gegen Zahlung eines Lösegelds soll dann der rettende Schlüssel zum Entschlüsseln wieder zugesandt werden. Bekannte Beispiele des letzten Jahres sind WannaCry oder Emotet. Wannacry hat weltweit ca. 230.000 Systeme in 150 Ländern befallen. In Deutschland war zum Beispiel die Deutsche Bahn betroffen. Anzeigetafeln auf den Bahnsteigen und Ticketautomaten hatten den Geist aufgegeben. Kleinere Krankenhäuser waren betroffen, aber auch mittelständische Firmen.

Kann ein gezielter Hacker-Angriff eine gesamte Infrastruktur lahmlegen?
Natürlich. Wir reden in Deutschland von sogenannten kritischen Infrastrukturen, wie der Energieversorgung, Telekommunikation, Logistik und Verkehr oder die medizinische Versorgung, um einige zu nennen. Wenn versierte, gut ausgebildete Hacker diese Infrastrukturen angreifen, kann es zum Ausfall bis zum Totalausfall kommen. Diese Möglichkeiten sind heute wahrscheinlicher denn je. Als warnendes Beispiele ist der Blackout in der Ukraine in den Jahren 2015 und 2016 zu nennen, wo mehrere 100.000 Haushalte ohne Strom waren.

Richten sich Hackerangriffe verstärkt gegen Institutionen oder gegen private Geräte?
Beides. Private IT-Geräte sind sicher nicht das Hauptziel von Hackern, die ordentlich Geld machen wollen. Gestohlene Bank-Accounts, TANs oder Kreditkarten sind die Beute. Aber auch hier sind die Schäden natürlich schon beträchtlich. Mehr Geld lässt sich verdienen, indem man Firmen oder Organisationen erpresst. Lukrativ ist auch, gefundene Schwachstellen bei Firmennetzwerken oder Software im Darknet, also dem digitalen Schwarzmarkt, zu verkaufen.
Ferner ist in jüngerer Zeit ein enormes Wachstum von mobiler Malware zu verzeichnen (50% pro Jahr). Und das trifft dann alle Benutzer von Smartphones, also eigentlich uns alle.
Professionelle Hackergruppen haben wieder ganz andere Ziele im Visier, da geht es um das Lahmlegen von ganzen Industrieanlagen oder Börsenmanipulationen.



Jürgen Neuschwander in seinem Büro an der HTWG. *Bild: Oliver Hanser*

Welchen konkreten Bedrohungen sind Unternehmen ausgesetzt?
Beispielsweise Distributed Denial of Service (DDoS-) Attacken, mit denen man Server von Firmen lahmlegen kann, das ist insbesondere für das Online-Business natürlich mit erheblichem Schaden verbunden. Oder man droht mit dem Verlust des kompletten Datenbestands, da man sich schon seit längerem in die IT-Systeme gehackt hat und man jetzt nur noch das Kommando zum Löschen geben muss. Da kann man durch Zahlung eines entsprechenden Betrags ja vielleicht noch davonkommen. Die andere Seite ist, wenn es nur um Zerstörung von Daten und das Blockieren von Geschäftsprozessen geht, also um Cybersabotage.

Sind die Unternehmen in der Regel gut geschützt?
Ein zögerliches Jein. Große Unternehmen treiben hier erheblich mehr Aufwand als die mittelständische Industrie. In vielen mittelständischen Unternehmen kann oder will man sich eine eigene IT-Abteilung nicht leisten. Wir haben Untersuchungen, z. B. im Rahmen von Masterarbeiten bei solchen Firmen durchgeführt, mit dem Ergebnis, dass die IT offen wie ein Scheunentor war. Und das bei Firmen, die zum Teil Marktführer bei bestimmten Maschinen sind. Dann braucht man sich nicht zu wundern, wenn bei einer Industriemesse die chinesische Konkurrenz das gleiche Produkt zum halben Preis anbietet.

Wie lassen sich digitale Spuren verfolgen?
Ganz schweres Terrain. Das Problem, den Verursacher eines Hackerangriffs zu finden, ist nicht gelöst, zumindest, wenn es sich um professionelle Hacker handelt. Die digitale Forensik (siehe Kasten) kann in vielen Fällen helfen, weil viele Hacker eben nicht professionell arbeiten, da unterstützen BKA und Verfassungsschutz in Deutschland, aber bei professionellen Attacken ist man chancenlos.

In welcher Form sind private Nutzer von Angriffen betroffen?
Natürlich ist hier der Risikofaktor der Mensch. Phishing Mails mit entsprechenden Links auf manipulierte Webseiten oder Anhänge mit Trojanern sind täglich Brot. Hier hilft nur das kritische Umgehen mit Mails, deren Absender man nicht eindeutig identifizieren kann. Im Zweifel immer Löschen. Überlastung am Arbeitsplatz, Zeitdruck oder schlicht Neugier sind hier Faktoren, die den leichtfertigen Klick auf einen Link oder eine Datei begründen. Und das Ganze jetzt auch noch auf den mobilen Geräten.
Werden digitale Identitäten von Nutzern geklaut, merkt man dies nicht direkt, sondern zum Teil erst Monate später werden die Auswirkungen eines Datenmissbrauchs bekannt, indem das Kreditkartenkonto überzogen ist, dubiose Bestellungen in Online-Shops getätigt wurden oder gefälschte Finanztransaktionen bekannt werden.

Was passiert in der Zukunft, wenn wir alle noch mehr vernetzt sind?
Bei der zukünftigen Vernetzung geht es um das Internet der Dinge. Damit werden viele einfache Gegenstände smart und bekommen eine Netzschnittstelle. Dann sind Webcams, Lampen, Kühlschränke alle vernetzt und in der Regel schwach gesichert. Diese Schnittstellen werden dann ganz neue Einfallstore für Hacker sein. Das wird noch ein riesiges Thema werden.

Sollte man im Internet überhaupt noch mit Kreditkarte bezahlen?
Wahrscheinlich sind Ihre Kreditkartendaten sowieso schon irgendwo abgefangen. Ich selbst zahle in Einzelfällen auch noch mit Karte im Netz, aber man hat ein ungutes Gefühl dabei. Beim Online-Banking mit dem Tan Generator von vielen Banken ist man dagegen relativ sicher, das ist ja ein eigenes, abgetrenntes Gerät.

Sind eigentlich Fingerabdrücke eine Alternative zu PIN und Passwort?
Eine Alternative schon, aber natürlich lassen sich auch hier geeignete Maßnahmen finden, diese Hürde zu überwinden.

Wie sieht es mit der Sicherheit bei den Fitnessuhren aus, die heute modern sind?
Da gab es einen kuriosen Effekt. Die US-Soldaten in Afghanistan machten Frühsport und haben ihre Jogging-Routen mit Fitness-Trackern aufgezeichnet. Das Ausspähen dieser Daten von einem bekannten Server wurde zu einem akuten Sicherheitsproblem für die Soldaten.

Haben Sie Tipps, wie man bei privaten Geräten mit der Bedrohung umgeht?
Nur die banalen Hinweise, dass man möglichst schnell alle neuen Patches von Betriebssystemen und Apps einspielen soll, einen vorhandenen Virenscanner täglich aktuell halten und vor allem keinen Links folgen oder Anhänge öffnen soll, die man nicht kennt. Auch wenn die Aussicht vielleicht verlockend erscheint, wenn in der Mail ein „entfernter Verwandter" einen mit 500.000 Euro aus dem Erbnachlass beglücken will. Und natürlich Backups nicht vergessen.

Die Fragen stellte Sabine Schulz

Vortrag zum Thema Cyberkriminalität

Prof. Neuschwander gibt am **27. März** gemeinsam mit Walter Opfermann, Leiter der Abteilung Spionageabwehr im baden-württembergischen Landesamt für Verfassungsschutz, und Torsten Seeberg, Abteilung Cybercrime des Landeskriminalamts Baden-Württemberg einen Einblick in seine Arbeit.
Thema: „Cybercrime – eine Gefahr für Unternehmen".
Termin: Mittwoch, 27. März, 17.45 - 21 Uhr.
Ort: IHK Hochrhein-Bodensee.
Informationen: www.cyberlago.net
Die Veranstaltung ist für cyberlago-Mitglieder kostenlos, für Externe kostet sie 10 Euro Eintritt (Bezahlung an der Abendkasse). Aufgrund der begrenzten Teilnehmerzahl ist eine Anmeldung erforderlich.

Digitale Forensik

Bei der digitalen Forensik wird versucht, bei gehackten Systemen den Urheber festzustellen. Es gibt „Hackerschulen", die einen bestimmten Programmierstil haben. Die digitale Forensik untersucht den Code und in welchem Stil programmiert wurde, so dass man den professionellen Hacker zwar nicht identifizieren kann, aber zumindest definieren kann, aus welcher (geografischen) Ecke er kommt.