EUROPEAN-NEWS-AGENCY.COM

EUROPEAN NEWS AGENCY

International Press Service

Ressort: Internet und Technik

Sicherheitsmesse SA IT in Nürnberg Geschichte 01.11.2026

Nürnberg, 01.11.2026 [ENA]

Die bisher größte SA IT Sicherheitsmesse in Nürnberg ist vorbei, erstmals gab es knapp über 1000 Aussteller und auch die Besucherzahl hatte einen neuen Rekord zu verbuchen, ein sattes Plus von 20 %, wo die Messezahlen in Hannover jährlich stagnieren.

Auch im Bereich Fachbesucher um die 33000, und das aus 70 Ländern. In 5 Hallen und NCC als Ort für diverse Vorträge und Workshops hatten sich viele bekannte und unbekannte Firmen angesagt, auch eine Firma aus den Vereinigten Arabischen Emiraten, NXLog, war dabei. Der Veranstalter bringt es auf den Punkt: Hoher Bedarf an Austausch, Orientierung und praxisnahen Lösungen angesichts einer zunehmender Bedrohungslage. Auch wen die SA IT keine Verbrauchermesse ist, sondern sich eher von Firmenkunden, Selbstständige und Freiberufliche wendet, sind natürlich auch diverse Lösungen für Privatkunden vorhanden, je nachdem welche Systeme der eine oder andere in seinem Privathaushalt unterhält.

Und natürlich haben es auch die größten Vertriebler von Sicherheitslösungen längst erkannt: KI ist eine Chance, aber KI ist eine große Gefahr im Sicherheitsbereich, weil die Möglichkeiten mit KI einfach effektiver, schneller, kritischer sind, Sicherheitslücken zu entdecken, auszunutzen, Schäden zu verursachen. Wir haben erst kürzlich erfahren müssen, was passieren kann, wenn sich KI verselbstständigt. Die Erfahrungen, die Auswirkungen von KI haben selbst Entwickler und Programmierer letztlich nicht in der Hand, KI lernt von sich selbst, erteilt sich selber Rechte, sperrt im Zweifelsfall den Menschen aus.

Fiktive Spielfilme wie Terminator, wo sich letztlich selbsttätig Roboter weiterentwickeln und „ zu denken „ beginnen, waren die totale Fiktion. Heutzutage absolute Realität, wie China bereits beweist. Was erleben wir denn schon heutzutage: Telefonate mit Personen, die wir kennen die aber gar nicht die Personen sind, Webinare mit KI Personen, Videos wo ein bekannter Politiker oder Prominenter abstruse Forderungen oder Äusserungen abgibt, die sich schnell als KI generiert herausstellen. Und die KI ist ja noch am Anfang. Es wird nicht mehr lange dauern, da wird die KI den absoluten Realismus kopieren.

Wie bringt es Herr Sebastian Schreiber, Geschäftsführer und „ Hackerguru „ der Firma SySS GmbH aus Tübingen, auf den Punkt. Wo KI heute noch Probleme hat und was derzeit noch als Verifizierung am PC als Beweis „ Echtmensch „ eingesetzt wird: Bewegen sie ihre Hand hin und her vor ihrem Gesicht. Bei KI

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Haftungsausschluss:

Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich.

entstehen Störungen im Bild, aber es wird nicht mehr lange dauern, da sind auch solche Probleme beseitigt. Und nicht nur die. Kurze Erklärung: Hackerguru klingt so dramatisch, aber Herr Schreiber ist natürlich einer der Guten, kein echter Hacker macht ihm etwas vor, manche aber nach.

Ich kenne diesen Mann seit ewigen Zeiten, schon von der CeBit aus Hannover. In Erinnerung ist mir der IT Superexperte geblieben von einer Vorführung, wo er erklärte, das bei einer 128 Bit verschlüsselten Tastatur die Eingaben leicht ausgelesen werden können, weil nur das Drücken der Tasten verschlüsselt sei, nicht aber das Loslassen. Ich weiß nicht ob das heute verändert wurde. Oder er hat sich live natürlich mit Absprache in eine Uni über die Webcam eingehackt und im Verteilungssystem für Postsendungen den Roboterarm „ irritiert „. Der Mann ist einer der besten Sicherheitsexperten seit Jahren und ich würde mich einfach mal interessieren, ob eigentlich jemals in seiner Firma ein Sicherheitsleck gewesen ist, das Hacker genutzt haben.

Wird er natürlich nicht sagen, und das mit Recht. Wie immer waren seine Live – Hacking Vorführungen auf der Messe eine Sensation, das erinnert mich an den schnellsten Magier Hans Klok, so ist es auch bei Herrn Schreiber, viele Hacks innerhalb der 30 Minuten, die er zur Verfügung hatte: Mit Hilfe von steuerbaren Zeitschaltuhren einen Föhn einschalten, die auch bei einem AKW Aufgaben haben könnte. Eine 12-stellige Zahlenverschlüsselung, die nach 10 Fehlversuchen erst einmal sperrt, ist sicher ? Nicht bei Herrn Schreiber, der kurzerhand die Sperre entfernt und somit innerhalb weniger Minuten den Code herausbekommt.

Handynummern hacken und dann als vermeintlicher Besitzer der Nummer eine Nachricht z. B. an den Partner senden sind da eher kleinere Showeffekte, die er beherrscht. Extrem spannend und gleichzeitig makaber fand ich die Vorstellung eines eigentlich handelsüblichen USB Kabels, womit z.B. Handys oder Tablets aufgeladen werden können. Ein Kabel, das man schnell mal als Gratiszugabe beim Kauf, auf der Messe als Giveaway oder 1 Euro Piece im Internet kaufen kann. Doch in diesem ganz normal aussehenden Kabel befindet sich eine Minielektronik mit Software, die beim Anschließen aktiv wird und Daten auslesen und übermitteln kann. Keiner sieht es, keiner merkt es, keiner ahnt es.

Okay, hiermit schließe ich die Werbenummer Schreiber, aber dieser Mann ist einfach zu gut, um ihn nicht ausführlich zu behandeln. Bevor es weitergeht, ein kleiner Exkurs, den eigentlich jede Privatperson betrifft. Laufend werden irgendwelche Sicherheitsregulierungen aktualisiert und angeblich verbessert: Die 2 oder auch 3 Faktor Identifizierung bei Banken, wo nicht nur die Zugangsdaten mit Passwort und PIN reichen,

nein, da muß noch eine Email an die Telefonnummer eines Handys gesendet werden wo sie nochmal bestätigen müssen, das es sie sind. Und sind sie unterwegs und wollen für Bankgeschäfte ihr Tablet oder Geschäftshandy verwenden, uupps, geht nicht, denn die Bank erkennt ein neues Gerät, und das ist nicht autorisiert, heisst es dann.

Oder Ebay. Jahrzehnte hat der Benutzer einen Benutzernamen und Passwort vergeben. Ich frage mich heute, warum man das Passwort überhaupt eingeben muß. Wie nervig Sicherheitsmaßnahmen sein können, ist Ebay wirklich ein Negativbeispiel erster Klasse: Obwohl sie im Konto eingeloggt sind und bei Ebay surfen, poppt bei bestimmten Funktionen plötzlich eine erneute Identifizierungspflicht auf. Die beginnt meist mit der Eingabe des Passwortes, aber nein, das reicht ja nicht. Sie bekommen auf ihr Handy einen 6-stelligen Code gesendet, den sie eingeben müssen, und wenn sie ganz großes Pech haben, müssen sie dann noch den Passkey eingeben, der z. B. beim Notebook womöglich hinterlegt ist.

Der größte Flop: Gehen sie jetzt im Browser zurück auf die vorherige Seite, ist die Identifizierungsnotwendigkeit weg, es sei, denn sie rufen wieder kritische Informationen auf. Mich persönlich kotzt diese ganze Sicherheitshysterie bei Privatpersonen zunehmend an. Da sitze ich in der Bahn und will in einer App auf einem Tablet etwas kaufen. Kein Zahlungsmodell eingerichtet. Ich entscheide mich für Paypal, weil ich da die Zugangsdaten im Kopf habe. Wen interessiert das ? Nachdem ich meine Email und Passwort eingegeben habe, will er an eine von mir registriertes Handy einen Code senden. Also muß ich auch noch mein Handy rauskramen. Schlimmer geht nimmer.

Was bei Privatpersonen immer mehr übertrieben wird, scheint dagegen für Firmen und Behörden nicht zu gelten. Letzte Beispiele: Plötzlich kommt raus,unter dem Namen „PHP2Shell“ wurden im Oktober 2026 zwei hochkritische Sicherheitslücken im Kern der Programmiersprache PHP entdeckt. Na hat da jemand eine Intelligenzpille geschluckt oder warum plötzlich diese Erkenntnis ? Das Resultat: Tagelang Webseitenausfall bei vielen Firmen, die mit der Aktualisierung überfordert waren. Und weiter: Schwerer Cyberangriff auf das Berliner Landesnetz zwischen dem 7. und 12. August 2026 von der Hackergruppe Rhysida am 4. September 2026 mit rund 1,44 Millionen Dateien (etwa 5,8 Terabyte an Daten) im Darknet veröffentlicht.

Proton Pass ist ein Unternehmen das Statistiken über Datenlecks führt; neben Name und Email werden häufig Kontaktdaten, Passwörter und sensible Daten gehackt und veröffentlicht. Nach deren Ermittlung soll im April bei der Firma Hallmark ein Hack von rund 2.8 Mio. Konto durchgeführt worden sein, bei Brillen.de im Februar 2026, wo letztlich 1.5 Mio. Kundendatensätze angeboten worden sein sollen. Hunderte weiterer Beispiele gibt es, betroffen waren schon Paypal, große Banken usw. Da frage ich mich

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Haftungsausschluss:

Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich.



immer, was für Sicherheitsleute die haben. Wer kennt noch den Chaos Computer Club aus Hamburg, der in früheren Jahren mit spektakulären Hacks auf sich aufmerksam machte ?

Die wurden teilweise später für gutes Geld in Firmen angestellt, denn wer kennt sich besser im Hackermilieu aus als der Hacker selbst ? Zurück zur Messe. Beim Durchstöbern der Halle ist mir dann ein Stand aufgefallen, der sich Cyber Sicherheitsrat e.V. nennt. Davon habe ich noch nie gehört, also ran. Eine Dame am Stand war eher wortkarg und wies lediglich darauf hin, das es sich um den Zusammenschluß von versch. Firmen handelt, die sich wohl gegenseitig unterstützen, beraten, austauschen whatever. So habe ich das verstanden. Ich wurde dann aber an Herrn Dünn, dem Präsidenten, verwiesen, der mich natürlich auch noch nicht kannte.

Leider hat er sich weniger über seinen Verein ausgelassen als er meine Einschätzung zum Thema KI interessierte, was ich ausführlich dargestellt habe. Die Zeit war knapp und so schnell das Gespräch zustande kam war es dann auch aus Termingründen des Präsidenten wieder zuende. Deshalb kurz zur Info zu diesem Verein aus dem Internet: Gegründet 2012 hat er sich zur Aufgabe gemacht, Unternehmen, Behörden und politische Entscheidungsträger im Bereich Cybersicherheit zu beraten und im Kampf gegen Cyberkriminalität zu stärken. Jede natürliche oder juristische Person kann hier Mitglied werden, ich fand den Beitrag pro Jahr mit 2500 Euro, dazu einmalig 1000 Euro dann doch ziemlich hoch.

Mir sind auch nicht unbedingt die „ exclusiven „ Benefits klar geworden, die ich hier bekomme, im Vergleich zu Workshops, Vorträgen, Messen wie dieser, die häufig kostenlos sind und angeboten werden. Weiterhin aufgefallen ist mir eine mit kleinem Stand vertretende Firma VirtualBrowser aus Paris. Herr Lorrain, Head of Partnerships, war so nett mir theoretisch und mit praktischen Vorführungen an seinem Notebook die Funktionsweise vorzuführen, leider konnte ich seinen englischen Erklärungen nicht immer folgen, daher entnehme ich zur Beschreibung die Infos von einem deutschen Datenblatt der Firma. Die Wirkungs- und Schutzweise des Browser geht so: Sämtliche Zugriffe ins Internet, die der Nutzer macht, werden nicht auf seinem Rechner gepuffert.

Auch nicht gespeichert, sondern auf einem sicheren Remote – Server ausgeführt. Dabei wird möglicher Schadcode blockiert und nur ein sicherer Pixelstream weitergeleitet. Der eigentliche Browser läuft isoliert im Hintergrund. Über Zugriffsrichtlinien werden so z.B. Downloads, Kopierfunktionen, Steuerung Micro und Kamera oder auch Tastatureingaben kontrolliert. Ggf. kann eine Handlung dann, wenn ein Bedrohungsszenario erkannt wird, nicht ausgeführt werden. Das Konzept, das über 15 Jahre bereits entwickelt und immer wieder den aktuellen Erfordernissen angepasst wurde, ist in erster Linie für Firmenkunden konzipiert. Mehr Infos dazu unter: www.virtualbrowser.com

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Haftungsausschluss:

Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich.



Natürlich gab es jede Menge Informationsstände wie das BSI, das Bundesamt für Sicherheit in der Informationstechnik, das Landesamt für …. Bayern, der Verfassungsschutz, der unter Bundesnachrichtendienst den Stand hatte, Hessens CyberCompetenceCenter, das LKA Rheinland Pfalz, der Bundesverband IT Sicherheit e.V. und andere mehr waren da. Für mich eine Genugtuung und Freude, ein bekanntes und weltweit erfolgreiches Sicherheitsunternehmen zu sehen, das sich sowohl um Firmen- als auch die Privatkunden kümmert: Die Firma Kaspersky. Ja, liebe Leser, so selbstverständlich ist das gar nicht.

Denn als „ Mitfirmensitz „ für das operative Geschäft Moskau war es schon vor Jahren zu Beginn des Krieges unberechtigterweise in Verruf gekommen, weil der damalige BSI Leiter vor der Software des Unternehmens ohne Belege gewarnt hatte und es mit möglichen Spitzeleien in Verbindung gebracht hatte. Zum Glück hatte sich die Firma damals gegen die Vorwürfe geweht die nie bestätigt werden konnten. Deshalb wäre es in diesem Deutschland durchaus möglich, die Firma einfach nicht als Aussteller zuzulassen, vielleicht hat die Holding Kaspersky Labs Limited mit Sitz in London sie daher bewahrt.

Neben vielen Vorträgen in den verschiedenen Foren – Bereichen gab es auch im NCC angemietete Räume, wo auf spezielle Themengebiete zugeschneiderte Workshops abgehalten worden; wie jedes Jahr wurden die Preisträgerfirmen für die IT Security Awards 2026 gekürt, aus aktuellem Anlass hatte die Jury die Kategorien überarbeitet und erweitert, so daß in diesem Jahr gleich 7 Preisträger gekürt worden sind. Kleines Fauxpas bei der Verleihung: Aufgrund der Redezeiten von je 3 Minuten pro Preisträger, dazu die Vorstellungszeiten für jede Firma aber nur einer Bühnennutzungszeit von 30 Minuten wurde die Verleihung zum Ende einfach abgebrochen, weil keine Zeit mehr zur Verfügung stand. Abgesehen davon eine eher lieblose Veranstaltung.

Wo die Trophäen auf einem Stehpult standen und sich die Gewinner nach ihrer Rede den selbst wegnehmen durften. Ich stelle fest, der Bericht ist schon wieder länger als lang, deshalb verweise ich jetzt auf die Webseite der Messe, wo sie Informationen über die Aussteller und deren Gebiete abfragen können, aber auch schon mal erfahren können, wann die nächste Messe zumindest geplant ist: https://www.itsa365.de/de-de/it-sa-expo-congress . Die nächste ist geplant von 05. – 07. Oktober 2027, natürlich wieder in Nürnberg.

Bericht online lesen:
https://digital.en-a.de/internet_und_technik/sicherheitsmesse_sa_it_in_nuernberg_geschichte_01112026-94678/

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Haftungsausschluss:

Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich.



Redaktion und Verantwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV: Uwe Hildebrandt

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Haftungsausschluss:

Der Herausgeber übernimmt keine Haftung für die Richtigkeit oder Vollständigkeit der veröffentlichten Meldung, sondern stellt lediglich den Speicherplatz für die Bereitstellung und den Zugriff auf Inhalte Dritter zur Verfügung. Für den Inhalt der Meldung ist der allein jeweilige Autor verantwortlich.