FÜR CYBERSICHERHEIT SORGEN – ABER WIE?

FOTO
© SEC Consult

ULRICH FLECK
Geschäftsführer SEC Consult

„Die Bedrohungsszenarien im Cyberspace wechseln ständig. Das Aufdecken von Sicherheitslücken allein reicht für eine nachhaltige Sicherheitsstrategie nicht aus, die nächste Attacke über einen neuen Angriffsvektor folgt bestimmt. Deshalb werden ganzheitliche Strategien immer wichtiger, um die Cybersecurity und das Problembewusstsein rund um das Thema Datensicherheit und Datenschutz in Unternehmen und Organisationen langfristig zu erhöhen. Dazu gehört zum einen, die IT-Sicherheit auf Herz und Nieren zu prüfen, zu verbessern und auf potenzielle Attacken bestmöglich vorzubereiten. Zum anderen braucht es dazu das Know-how, um im Ernstfall den Angreifer auch rasch erkennen und sofort entsprechende Verteidigungsmaßnahmen ergreifen zu können, sodass der Schaden möglichst gering gehalten werden kann."

FOTO
© Kurt Goethans

KARL PICHLER
CEO der InnovaticGroup &
Veridium-Vertriebspartner in Österreich

„Meiner Meinung nach gehört der KI-basierten Verhaltensbiometrie die Zukunft, um eine sichere Authentifizierung im Cyberspace zu gewährleisten. Denn im Gegensatz zu klassischen biometrischen Lösungen wie Gesichtserkennung oder Fingerscans wird nicht nur ein charakteristisches Merkmal für die Authentifizierung herangezogen, sondern das gesamtheitliche, individuelle Bewegungsmuster einer Person. Und je ähnlicher unsere digitale Identität unserer angeborenen Identität ist, desto sicherer werden die Anwendungen – denn das Duplikat eines realen Menschen zu erstellen, wird noch lange Science Fiction bleiben."

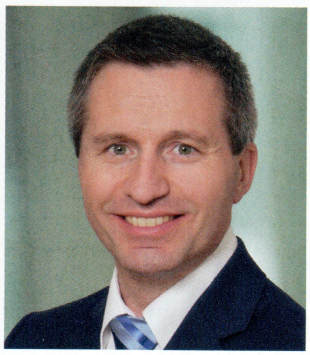

FOTO
© A-Trust

MARKUS VESELY
Geschäftsführer A-Trust

„Grenzenlose und sichere virtuelle Interaktionen quer durch Europa benötigen vertrauenswürdige digitale Infrastrukturen, damit Länder und Regionen als Wirtschaftsstandort international wettbewerbsfähig bleiben. Datenschutz, Datensouveränität, Rechtssicherheit und Schutz des geistigen Eigentums gehören zu den wichtigsten Bausteinen erfolgreicher wirtschaftlicher Entwicklung und gesellschaftlicher Teilhabe. Sichere digitale Authentifikationslösungen sind ein wichtiger Baustein dafür."

FOTO
© CYBERTRAP/
Sabine Penz

FRANZ WEBER
Geschäftsführer CYBERTRAP

„IT-Sicherheit muss man im Grunde als laufende Investition betrachten. Die Branche entwickelt sich stetig weiter, auch Hacker finden immer neue Wege, Lücken in den Systemen auszunutzen. Angreifer nutzen in der IT-Welt ständig das Element der Täuschung, sie geben vor, jemand anderer zu sein. Verteidiger nutzen diese Taktik noch recht selten, daher sehe ich viel Potenzial bei den sogenannten Täuschungssystemen, mit welchen eine gefälschte Kopie des eigenen Netzwerks erstellt wird. Hacker, die schon in System eingedrungen sind, kann man dorthin locken – wo sie nun keinen Schaden anrichten können."