Beat: News

CYBER WORLD CALLS FOR DISRUPTION

Change is on the Menu at RSA 2015

San Francisco, 23.04.2015, 05:31 Time

USPA NEWS - RSA2015 in San Francisco opened Tuesday with everyone sitting in the dark. No joke! Amit Yoran, the new president of RSA Security began his keynote while standing on a dark stage. "My stumbling around in the dark is a pretty good metaphor for anyone who's trying to protect networks today.

Very little doubt, the computer security industry is eating humble pie at this week's RSA Security Conference in San Francisco. Amid continued cybersecurity break-ins and a growing threat landscape, here are five key IT security and data protection trends emerging at the conference.

1. As far as That Humble Pie: Amit Yoran, president of EMC Corp.'s RSA unit, says the IT security industry has has failed because "organizations that are investing millions and millions of dollars in security" are "still getting compromised on a consistent basis," according to an interview with The Wall Street Journal. In a separate interview, Yoran told Fortune that it's time for "No More of the Same. Let's do things differently; let's think differently; let's act differently. Because what the security industry has been doing has not worked."

2. Every thing to Protect Intellectual Property: Richard A. Clarke, the former special advisor on cybersecurity to the U.S. President, issued a warning ahead of the conference -- stating that cybersecurity must increasingly protect intellectual property. He alleged that cyberattacks from China continue to steal intellectual property from the U.S., and will ultimately erase the United State's innovative edge in business.

3. Cybersecurity Has to go Vertical: While all industries are under attack, multiple vertical market organizations are pushing new cybersecurity recommendations. Just ahead of the conference, a list of 12 cybersecurity principles emerged from the The Cybersecurity Task Force of the National Association of Insurance Commissioners. The health care, financial services and manufacturing industries have also been developing a range of cybersecurity recommendations.

4. It's All About the People: Amid all the technical threats, most research still points to people -- your own employees -- as the single biggest IT security threat. Indeed, social engineering -- phishing email, fraudulent phone calls and more -- still trick employees into sharing personal and corporate information. Indeed, the 2013 Target hack likely started the moment a Target employee clicked on a phishing email, experts have stated.

5.Conclusion is that Holistic Approaches are Needed: Instead of betting on individual software and security companies, experts at the conference are telling attendees to take a more holistic approach to IT security. Figure out your overall threat landscape first, then begin to mix, match and integrate the best third-party offerings into a total solution

.

To add salt to injury, 82% of organizations expect a cyberattack yet 35% are unable to fill open security jobs global talent pool reflects urgent skills shortage and hiring delays. According to a study by ISACA and RSA Conference, 82 percent of organizations expect to be attacked in 2015, but they are relying on a talent pool they view as largely unqualified and unable to handle complex threats or understand their business. More than one in three (35 percent) are unable to fill open positions. These are the key findings of the State of Cybersecurity: Implications for 2015, a study conducted by ISACA, a global leader in cybersecurity, and RSA Conference, organizers of prominent, global cybersecurity events.

Among the smorgasbord of "new and notable": The Irish startup Waratek aiming to make enterprise solutions more secure, was named most innovative company 2015 @RSA and UK's Tvolution "#Becrypt“ a powerful, portable mini device, allowing for quick

and effective management of workspace for end users, through which they can access virtualized desktops or web-based resources. Not only does tVolution Mini provide a means to cope with short term disruptive effects for individuals, it also provides a disaster recovery option for more widespread emergency situations.

"Controllable Visual Hacking " a phenomena explained by CEO Larry Ponemon, as an "observational method used to train employees to protect against low tech threats" gives us some food for thought as does Versasec´s vSec ID whose Server provides a complete set of functions for digital transaction verification, thereby ensuring confidentiality, integrity, privacy, authentication and non-repudiation of online transactions. It is a PKI-enabled server component that supports several interfaces, such as HTTP, Web Services and SDK. It supports cryptographic, tasks such as encryption, decryption, signing, verification and certificate validation. It is highly scalable and is proven in major corporations and government organizations.

While starting in the "Dark", RSA 2015proved that there is "Light" at the end of the tunnel. Yet, we have to keep in mind that "Cyber is All About the Maybe" as Gary Hayslip, Deputy Director, CISO of the City of San Diego very astutely and perceptively pointed out.

Article online:
https://www.uspa24.com/bericht-3895/-cyber-world-calls-for-disruption.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Ina von Ber

Editorial program service of General News Agency:
United Press Association, Inc.
3651 Lindell Road, Suite D168
Las Vegas, NV 89103, USA
(702) 943.0321 Local
(702) 943.0233 Facsimile
info@unitedpressassociation.org
info@gna24.com
www.gna24.com