03.05.2019 | CYBERSECURITY TRENDS

HIGHLIGHTS AND LEARNINGS FROM THE RSA CONFERENCE 2019

The RSA conference is one of the world's biggest IT security event held yearly since 1991. This year, the meeting took place from 4 to 8 March in San Francisco and attracted more than 40'000 attendees and more than 600 suppliers of cybersecurity solutions. Crypto's Cybersecurity Consultant attended the event. Here are some of his reflections.

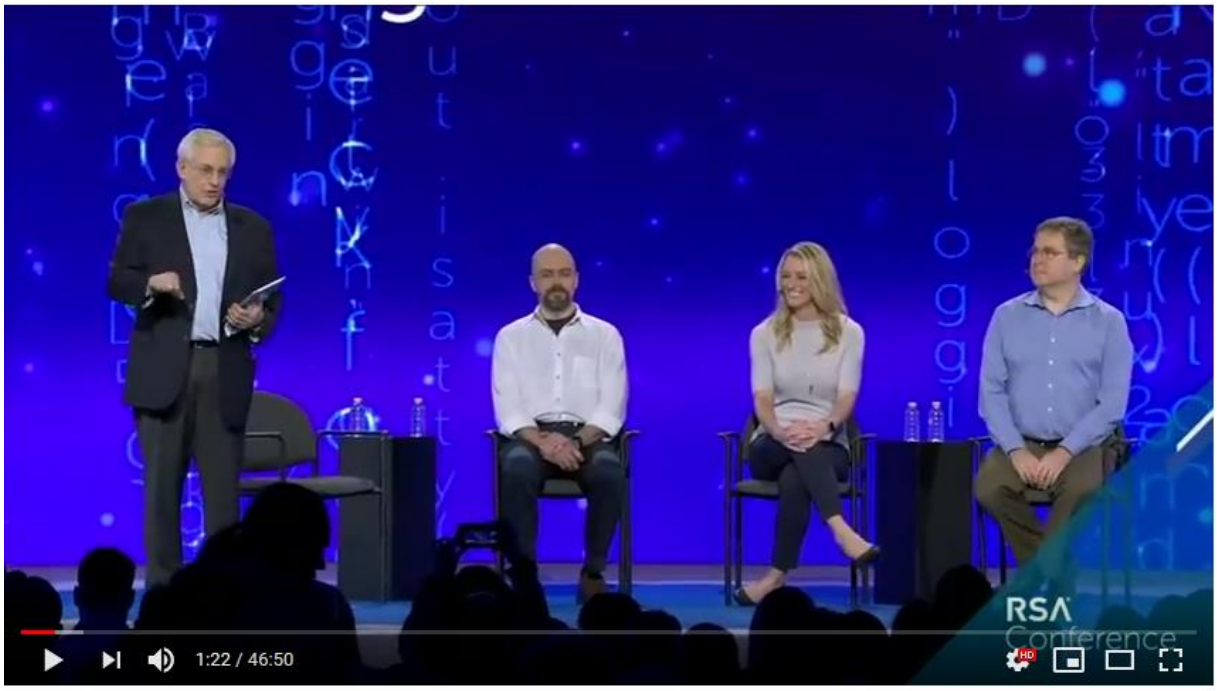
The theme of this year's conference was "Better", which resonates with better and stronger security solutions and infrastructure, as well as more efficient IT security teams. In our era of global attacks and breaches, these aspects are more important than ever.

A plethora of products

Microsoft's keynote showed that the cybersecurity industry so far has laid the emphasis on creating more and more products instead of focusing on the fact that security should be built in from the beginning and that security should be guaranteed in the overall system. The learning is that higher security does not come from the use of a collection of shiny products but relies on competent people able to provide a comprehensive solution to each specific situation. To reduce the risk of successful attacks to a minimum, methods and procedures must always be aligned.

New attack techniques and how to counter them

Different experts gathered around Alan Paller, Research Director and Founder (SANS Institute) to share their latest experience and give insights into the threats that have developed over the last couple of months.



The Five Most Dangerous New Attack Techniques and How to Counter Them
You can view the whole presentation on YouTube: (Picture: RSA Conference / YouTube)

Here is a brief summary of the most important learnings.

DNS manipulation

The manipulation of DNS records enables attackers to redirect e-mails and register fully accepted TLS certificates. Since many certificate issuers only check that you can click on a link in an email to verify that you own that domain the attackers are able to register a new valid certificate to use on a site set up by the attacker.

- Look to use only DNS-certificate from sources that use two-factor authentication
- Implement DNSSEC
- Monitor any changes to certificates on your sites
- Revoke bad certificates immediately

To do this, it is indispensable to collect information from the SOC or another organization to find out about any announcements of DNS updates on your domains.

Domain Fronting

This is a type of attack targeted at cloud services that you use for your business as customer. The attackers exploit the fact that different cloud suppliers need to trust each other, otherwise their services would not be able to work together. The attackers get an account on the same CDN (Content Delivery Network) and use that service to attack you. The truth is that this procedure is quite simple for hackers and that it hasn't been fixed yet. It a very effective way for attackers to hide the command and control channel in order to exfiltrate the compromised data.

The attackers' main trick is to obscure where they are coming from. Unfortunately, most organisations trust the data traveling to and from their own cloud provider and forget that other users of the same cloud service could be evil. If one cloud provider decided to filter out the attackers, it would be easy for them to hop from one cloud to the next and finally disappear in the fog.

Countermeasures to address Domain Fronting:

- Use enterprise TLS interception at network borders
- Do not automatically trust traffic going to and from your cloud provider
- In your risk assessment, also consider scenarios where your cloud provider is compromised

The Dutch Cybersecurity Centre has compiled an excellent guide on TLS interception. Black Hills' free Real Intelligence Threat Analytics (RITA) tool can spot beaconing through Domain Fronting.

The shift to data at rest

With companies and state agencies collecting huge amounts of data, the interest for the security of stored data is growing. The large number of attacks against data at rest either at data centres or on cloud services shows that this new emphasis is of vital importance.

Here are some simple measures that can easily be implemented to improve general security:

- Encrypt logs and keep the private key in cold storage, never keep the private key on the system. If your system gets breached, you can dig out the key and check if you believe that you have been compromised. The logs that are encrypted tell the truth.
- Password-authenticated key exchanges (PAKE)
- Multiparty computation and Threshold signing to renew SSL certificates

- Systems connected to the internet should use DNSSEC and TLS 1.3
- When developing new systems, use modern programming languages that provide a good basis for security. One great example is the RUST programming language.
- Turn away from password only security and use cryptographic authenticators
- Check that the encryption you use is quantum-safe!

Learn more about the RSA Conference and watch the videos of numerous talks on: www.rsaconference.com

For more information on Crypto, visit: www.crypto.ch

For your cybersecurity issues, talk to Crypto's experts: crypto@crypto.ch