DeepINTEL Conference approaches the next generation of IT Security

Posted on **August 31,2017** by **sanna**

Strategic Information Security: Predicting the Present

DeepINTEL Conference presents Approaches to the Next Generation of Security

Many products and approaches of information security are trying hard to predict the future. There is always a lot of talk about threats of the future, detection of attacks before they arise or the magic word "pro-active". But the prediction of the future does not benefit your business if the present is still unknown. When it comes to information security this means: Do you now know enough about your current situation to make the right decisions within the next few hours? The DeepINTEL seminar conference, which takes place on 21st/22nd of September in Vienna, focuses on this strategic question.

Analogies distort Perception and Facts

Analogies are often used to illustrate connections. Especially in the areas of IT security, people use a lot of terms from the military sector. “Attack” and “defense” suggests this kinship, but this wording automatically evokes assumptions that are not met. Errors in communication protocols, code, program crashes, or hardware peculiarities are not weapons, no matter how much you stretch your imagination. You can not armour Internet accesses. There are also no bulletproof databases or mailboxes. The analogies quickly break down and obscure what is actually going on - What information about your own infrastructure and communication is available, and what does this data mean in terms of real risks? This knowledge can not simply be bought from service providers, you have to gather it through experience in your own field of business. Companies know their own processes very well, and this knowledge must be integrated into their IT security.

Security Intelligence as a collection of methods

In the media or in advertisements the term security intelligence very often has a different meaning. For security experts “security intelligence” means the knowledge of methods that can be used in an attack, the knowledge of the capabilities of the attacker, and the analysis of open source intelligence in the context of the expected risks. In concrete terms, this means to point out the means used against an organization, which must be neutralized or mitigated by its IT security. This also includes threats outside of technology, internal threats, the search for the right personnel, secure communication behaviour and much more. Security intelligence as a process is the necessary first step before you can start to implement, even begin to discuss security measures. For this reason, companies are hardly concerned with it and rely on external suppliers. DeepINTEL wants to offer you the opportunity to get acquainted with this topic. Some companies have successfully set up their own security intelligence teams, or at least developed methods to not build digital access barriers blindly. Ultimately, your IT security measures become more secure and more accurate.

In particular, areas such as critical infrastructure (energy supply, networks), finance, insurance, transport (freight forwarding companies, public transport, airports), health care or public authorities can benefit by adapting their digital defence to the very risks, they have to face.

Interactions are everywhere

An important topic DeepINTEL focuses on are interactions. In terms of security interactions between people or machines (in any combination) are always critical. No successful attack can do without them. At DeepINTEL presentations will focus on the manipulation of human action, on motivations and the profiles of internal aggressors, as well as on the influence of human memory and the role of propaganda in geopolitical conflicts.

We started out by explaining how important information is – but let's not underestimate the role of disinformation. It is an important tool of all opponents in information security. The human factor gets passed over way too often – Personnel departments can't be protected only by technical means. Who effectively wants to attack an organization will try to infiltrate and place their own personnel inside the company. One must not forget: Really effective attacks are prepared for months or years. There's enough time to hire an accomplice or to persuade or blackmail an employee to become an internal threat. Such preparations can't be traced within the logs of servers and applications: who relies on technology only to defend themselves against attacks are badly prepared.

But of course the technical aspect of IT Security will also be in focus of this years DeepINTEL: The conference features talks about the profiling of malicious software, the weak points of the power supply network, the failure of industrial control systems (SCADA) and human errors related to secure communication systems. Unfortunately there is no area of ??modern infrastructure where you do not have to look for security gaps. The results presented are derived from actual incidents and real-life security tests - and present a good opportunity to think about setting up your own case studies aided by real information. Such business games are beneficial, just like fire drill exercises, and they help to build up realistic scenarios that your digital defense needs to consider.

DeepINTEL Programme and Registry

Who wants to get into the future undamaged, must master the present. To use misguided analogies one last time: You can win every battle in the digital world and still lose the war. To escape this fate, sign up today to the DeepINTEL conference. There are still a few discounted tickets from the sponsor's contingent. Contact us and get the booking code - better today then tomorrow.

The current program can be foundat the DeepINTEL web site.

You canregister directly at the DeepINTEL web site.

Posted in:Conference,Discussion,Security Intelligence | Tagged:Conference,DeepINTEL,Programme,Security Intelligence | With 0 comments