Digital Security of the Future: Technology and Algorithms alone are no Substitute for Strategy

Posted on **July 14,2017** by **lynx**

Unfortunately, you can not rely on antivirus programs when it comes to the security of your own business. Antivirus programs do not read newspapers, they do not attend lectures, they don't protect you from social engineering or know the meaning of Facebook friends or Twitter tweets. False friends, indeed.

The continuous monitoring and evaluation of threats is the next step in information security. This aspect has always been an important part of digital defense. Today's discussion often centers around the term Security Intelligence, which unites different approaches. The DeepINTEL is Austria's first event, which, since 2012, has been taking up this topic - in all its facets, because modern information security is interdisciplinary. Lectures by experts from various fields of science, defence and industry: At DeepINTEL you have the opportunity to strategically rethink your digital protection and improve it decisively.

Internal Threats are often underestimated

The most dangerous threats come from within. That is to say, if modern companies can still distinguish between internal and external at all – social engineering is a dangerous threat, which overcomes any technological barrier. Mostly unintentionally, but in the case of targeted attacks long prepared and deliberately, actions lead to compromised systems or information to be inserted or removed. The presentation of Professor Ulrike Hugl is devoted to classifying internal threats according to motivation and behaviour. Profiles based on current cases will be presented and discussed. From this, you can derive methods for your own defence.

Real-time is no longer good enough

Analysing threats and reacting in real time is no longer enough. Who's just on a par with the attacker can't prevent damage. This is true for almost all protection systems currently used in companies and public authorities. An effective defence requires several ways to anticipate the next steps of the opponents and to take action against them in a targeted and coordinated way. Only a few manage to take the next step forward towards the use of adaptive measures. At DeepINTEL, Matthias Seul, an expert from the IBM Protector team will analyse the facts and share his experiences.

Telltale Metadata and Behavioural Patterns

Measurable relationships between entities and behaviour patterns of actors are key information for threat analysis. With ProcDOT, Christian Wojner is presenting a tool in his DeepINTEL lecture that uses malicious software to draw conclusions from the behaviour of the code and compare it. A visualisation based on time stamps and graphs is used, which composes thousands of individual activities into one overall picture. Compared to classical methods this information is much more meaningful because cross-connections between variants of malicious software and activities become visible. The analysis of social networks achieves something similar. Using the example of Twitter there'll be an impressive demonstration at DeepINTEL on how to visualize the data flow between and the networks of various groups using publicly accessible information (Open Source Intelligence, OSINT). The principle can be applied to the entire spectrum of social media.

Disinformation and Cyber War

Any dispute uses disinformation as a weapon, no matter whether the opponents oppose each other analogously or digitally. The outbreak of the Petya.2017 virus is a good example. The malicious software was never meant to be ransomware. Rather, its aim was to achieve media attention and to spread a specific story. At DeepINTEL Volker Kozok will talk about another highly topical example: He discusses elements of the Russian cyber war strategy by means of the Russian and Ukrainian activities in networks. The borders between cybercrime, hacktivism, and state sponsored actions are blurred, making an easy assignment, as it is portrayed in the media, very difficult. The lecture also illuminates the narratives and Russian propaganda, as they are disseminated in Germany, as well as the role of online trolls and social bots.

Unfortunately, when it comes to information security, a company can not shut itself off from geopolitical events. Antivirus programs do not read newspapers nor attend lectures, so the importance of security events must be taken into account by the IT department.

Seminar Conference

The DeepINTEL conference aims to provide a platform where both experts and users can share and exchange ideas about methods of security intelligence. Modern information security is interdisciplinary because it is about so much more than electronic data processing like back in the 1960s. Delegation in the form of outsourcing only shifts problems and makes you blind to threats. At DeepINTEL you have the opportunity to strategically rethink your digital protection and improve it decisively.

The DeepINTEL conference takes place on 21/22. September 2017 at the Imperial Riding School – A Rennaissance Hotel in Vienna. The preliminary schedule is also available for download.

Posted in:Conference,Security Intelligence |
Tagged:Announcement,Cybercrime,Cyberwar,DeepINTEL,SecInt,Security,Strategy | With 0 comments