Contribution ID: **162** Type: **Paper**

Insider threat and computer security: is there a specific profile?

In the infosec community, insider threat is a "buzz word"which covers several different meanings. However, in the nuclear field, IAEA has precisely defined it as "an adversary with authorized access to a nuclear facility, a transport operation or sensitive information".

Because many functions in nuclear facilities are now digitalized, computer networks are natural targets for a malicious actor and the agency's definition of an insider can be applied to computer security.

In that aspect, "authorized access"can be broken down into two distinct domains:

- Physical access to a network equipment.
- Logical access to accounts/network functions.

Of course, to be able to generate a significant impact like a major denial of service, extraction of sensitive data or takeover of the industrial process, an adversary must gain a high level logical access (in technical terms, he basically needs at some point to become "root"or "admin"), hence the widespread belief that insiders, in the computer security field, must have a deep computer and network knowledge and a high level of access rights, which can only be found in a small group of IT specialists like administrators, architects, maintenance or computer security engineers.

Of course, insiders could be found in this population but real life has shown something very different.

By analyzing TTP's (Tools, Techniques and Procedures) of cyber attacks, some use cases with insiders can be highlighted.

Indeed, cyber attacks on critical or high value network, which are more and more protected require alternative means to bypass defensive measures. For targeted attacks like Advanced Persistant Threat (APT), which are interactive and extend over a long period of time, a group of attackers will gain entry by any means in the network and from there, will discreetly study it, execute reconnaissance and adapt their attacking tools to gain better logical access until they reach their goal and strike.

The threat actor, when confronted with an air gap or a very well hardened network, will have difficulties to penetrate the outward perimeter, he will thus tend to use an insider to get first a physical access to the network, primarily to establish a covert communication channel (either through the Internet or by another means) with the main team waiting discreetly and anonymously outside the network. He will then proceed to the following steps of the attacks by escalating privilege and moving laterally, without the insider's help.

In that case, the insider has just a very basic and one-time role to plug a device or execute a single action, the rest of the attack will be conducted from elsewhere thanks to the remote connection.

In fact, he doesn't need to know computer science or to have technical knowledge, he just needs to have a physical access to a network device.

In conclusion, insider threat covers a short but essential and critical phase in the overall computer attack and there is indeed no specific profile for insider in computer security.

We should consider two criterias when assessing this threat:

- Physical access to an element of the network with which an insider can interact. That could be an endpoint, switch, firewall…. or a simple ethernet plug.
- Possibility of setting up a covert communication channel with the outside world. It should be noted that the second criteria is not necessary if the opponent has an exhaustive knowledge of the targeted system and is able to program an autonomous malicious code.

Gender

Male

State

France

Author: Mr FICHOT, Olivier (IRSN)

Presenter: Mr FICHOT, Olivier (IRSN)

Track Classification: CC: Information and computer security considerations for nuclear security