CIONET

Infrabel

Infrabel managed, maintains and modernized the Belgian railway infrastructure. They coordinate the rail traffic on the Belgian network. They have 5 main priorities. Number 1 is Safety, then Trains that are running on time. Number 3 is the work on the train rails. 4 is a financially healty company and last a board with society.

Security challenges are

* Avalability: for the IT-systems with limited intervention windows
* Monitoring , support and incident management
* Geographic presence in the whole country

Made a risk assessment and a top 15 of security risks. Information security in Infrabel is now risk based.

Each of these security risks gets a global risk score and then they made a top 15

After terrorist attacks:

Strategic information security plan based on 7 domains and 26 actions. The board of Infrabel approved this security plan on 17 March 2015. The 7 domains are IT applications, ICT end Devices, ICT networks, Uniform controls, buildings, signaling, Human factor

FoxIT

Kill Chain

We will have to for future security

* Take security serious
* Simplify infrastructure
* Unify our security operations

! Do not clean to quickly: keep infected pc and see how it works. Come up with a cleaning plan (but you need the resources to do so). Not everybody gets the budget.

Attacker knows that there is monitoring so it will first monitor itself and see what the normal communication is. After that it will replay it and not do something different. So from the outside it is difficult to detect.

FCCU

A lot of targeted attacks that stay uncovered in a network. They will try to get inside as far as possible.

Overall learned lessons:

A lot of targeted attacks that stay uncovered in a network. They will try to get inside as far as possible.

Do not clean to quickly: keep infected pc and see how it works. Come up with a cleaning plan (but you need the resources to do so). Not everybody gets the budget.

If you are always in defense you will never win the game