Cyber-management : LABS

Risk analysis and countermeasures

Thibault Debatty

10/11/2017

Download this presentation

http://filetray.net/files/rucd

Risk assessment

- NIST SP800-30
- ISO27k
- SANS

Risk assessment

- system identification
- threat
- vulnerability
- likelihood
- impact
- risk (= likelihood x impact)

Risk assessment

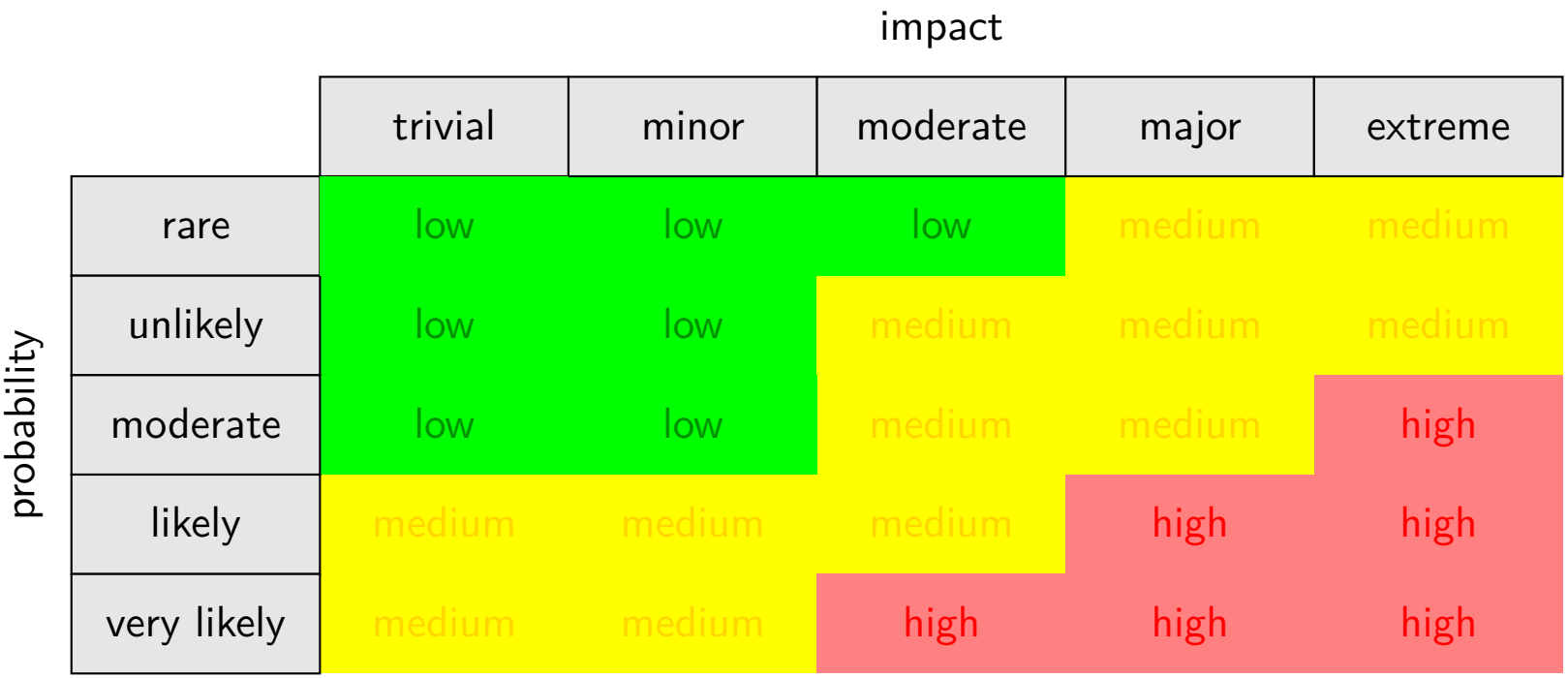

Figure 1: risk determination

Risk assessment

Impact:

- Confidentiality
- Integrity
- Availability

Risk assessment : example

Data diode availability:

- 5min = minor
- 30min = moderate
- 1h = major
- 4h = extreme

Risk assessment : example

- system: **login page**
- source: a **hacker who managed to get access the internal (unsecured) network of the client**
- threat: the hacker uses packet sniffing techniques to get the authentification credentials of the administrator
- vulnerability: credentials are sent over the network in clear

Risk assessment : example

- likelihood: as we have no view on the way the client secures the access to his network, we should assume that the event is **likely** to occur
- impact: the attacker would be able to shutdown the data diode hence compromising **availability** for 1h or more, which is considered a **major** impact
- risk: **high**

Countermeasure

- avoid
- mitigate
- transfer
- accept

Coutnermeasure : example

- avoid: the web interface must be available only through https
- transfer: the client is responsible for securing access to the internal network