Getting started with CRITICAL INFRASTRUCTURES

by Nicole Britz (Piratenpartei Bayern)

PIRATENPARTEI
Bayern

Intro

- Nicole Britz
- IT Infrastructure Specialist
- Specialized in web operations
- Chairwoman of Pirate Party Bavaria since October 2013

Synopsis

- What are critical infrastructures?
- What characterizes them?
- Can things get even worse?
- What could be done to make them less critical?

What makes an infrastructure critical?

Which household item could be critical in your everyday life?

Critical infrastructure @ home

More critical infrastructure @ home

What makes it critical?

- Institutions and organizations with important significance for the state community
- failure or impairment sustained shortage of supplies
- significant disruption of public security
- Are often linked and depend on each other
- can lead to risks and cascading effects

Possible threats

- Actual hacking (Sony)
- Special purpose malware (Stuxnet)
- Destruction / terrorist attacks (bombs etc.)
- Sabotage, Accidents
- Poisoning a/o radioactivity (water, air, food)
- War
- Whistleblowing
- Dysfunctional risk management and stupidity

Animals as successful hackers

Source: Engadget

Agent	Success
Squirrel	623
Bird	214
Racoon	52
Snake	47
Rat	25
Beaver	9
China	0
Russia	0
USA	1

Unavailability

- Cannot be used, even if urgently needed
- No backups or redundancies
- No or limited workarounds
- Time needed to restore / repair
- Dependencies

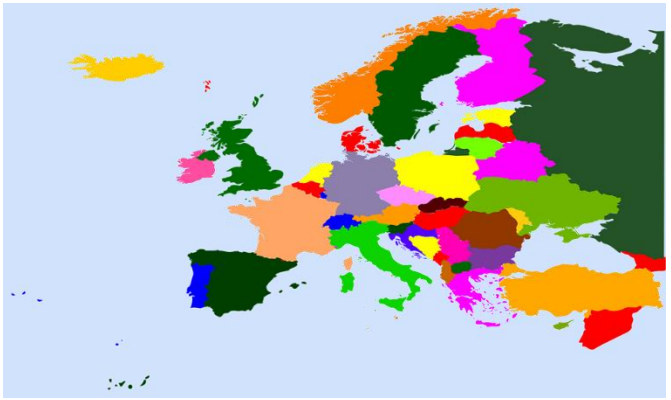
Information technology

- High availability setups very common
- Expensive
- Elimination of single points of failure

Availability %	Downtime per year	Downtime per month	Downtime per week	Downtime per day
90% ("one nine")	**36.5 days**	**72 hours**	**16.8 hours**	**2.4 hours**
95%	18.25 days	36 hours	8.4 hours	1.2 hours
97%	10.96 days	21.6 hours	5.04 hours	43.2 minutes
98%	7.30 days	14.4 hours	3.36 hours	28.8 minutes
99% ("two nines")	**3.65 days**	**7.20 hours**	**1.68 hours**	**14.4 minutes**
99.5%	1.83 days	3.60 hours	50.4 minutes	7.2 minutes
99.8%	17.52 hours	86.23 minutes	20.16 minutes	2.88 minutes
99.9% ("three nines")	**8.76 hours**	**43.8 minutes**	**10.1 minutes**	**1.44 minutes**
99.95%	4.38 hours	21.56 minutes	5.04 minutes	43.2 seconds
99.99% ("four nines")	**52.56 minutes**	**4.38 minutes**	**1.01 minutes**	**8.66 seconds**
99.995%	26.28 minutes	2.16 minutes	30.24 seconds	4.32 seconds
99.999% ("five nines")	**5.26 minutes**	**25.9 seconds**	**6.05 seconds**	**864.3 milliseconds**
99.9999% ("six nines")	**31.5 seconds**	**2.59 seconds**	**604.8 milliseconds**	**86.4 milliseconds**
99.99999% ("seven nines")	**3.15 seconds**	**262.97 milliseconds**	**60.48 milliseconds**	**8.64 milliseconds**
99.999999% ("eight nines")	**315.569 milliseconds**	**26.297 milliseconds**	**6.048 milliseconds**	**0.864 milliseconds**
99.9999999% ("nine nines")	**31.5569 milliseconds**	**2.6297 milliseconds**	**0.6048 milliseconds**	**0.0864 milliseconds**

Source: Wikipedia

How much redundancy do you need?



- Datacenters
- Computing environments
  1. Have a single server
  2. Have two synchronized servers
  3. Have two synced servers in different fire compartments
  4. Have them in different datacenters in the same city
  5. Have them in datacenters in different cities
  6. Have those datacenters in different countries
  7. Have those countries on different continents

Private infrastructure

- Power plants
- Factories
- IT Systems
- Websites
- (Sensitive) data
- privatized public infrastructure
- …

Public infrastructure

- electricity generation, transmission and distribution
- gas production, transport and distribution
- oil and oil products production, transport and distribution
- telecommunication
- water supply (drinking water, waste water, dikes and sluices
- agriculture, food production and distribution
- heating (e.g. natural gas, fuel oil, district heating)
- public health (medicine, hospitals, ambulances)
- transportation systems
- financial services (banking, clearing)
- security services (police, military)

Source: Wikipedia

How to improve vulnerability?

- Store large amounts of sensitive data in one place
- Cut budgets for security
- Public Private Partnership / Privatizing public infrastructure
- Weaken data protection policies
- Be unaware of risks (or ignore them)
- Make stupid decisions

Data thrift (Datensparsamkeit)

Alexander Dobrindt

Federal Minister of Transport and Digital Infrastructure

The policy of data thrift must be abandoned for the sake of big data and „data wealth“ (Datenreichtum).

No more cash?

- Abolition of cash money
  - trace terrorist money
- Virtual money only
- What will happen if infrastructure fails?
- Make a vulnerable infrastructure even more vulnerable
- And: Complete loss of privacy

Issues with

Possible threads:

- Hacking, sabotage, theft, power outages
- The government will know, that you bought a loaf of bread on 27th March 2018 at 7:26 a.m.

- Effects:

  You can‘t buy a loaf of bread when your money is offline.

- Solutions: Keep the cash

Electronic HealthCard

Die elektronische Gesundheitskarte (eGK)

Issues with

- Central data storage of name, address, medical findings, medicine prescriptions etc.
- Scenario:
  - Hacking, weak data protection laws, weak encryption, human error, sabotage
- Solutions:
  - don‘t do it, strong encryption, decentralization

Other future risks

- Self driving cars
- Remote surgery
- Genetic code
- Individual health information (Blood type, genetic disorders)
- …

Questions? Comments? Concerns?

nicole.britz@piratenpartei-bayern.de