Day 4-1-5

Wipe, Recover, Replace, Archives Remote fallback

action plan to recover

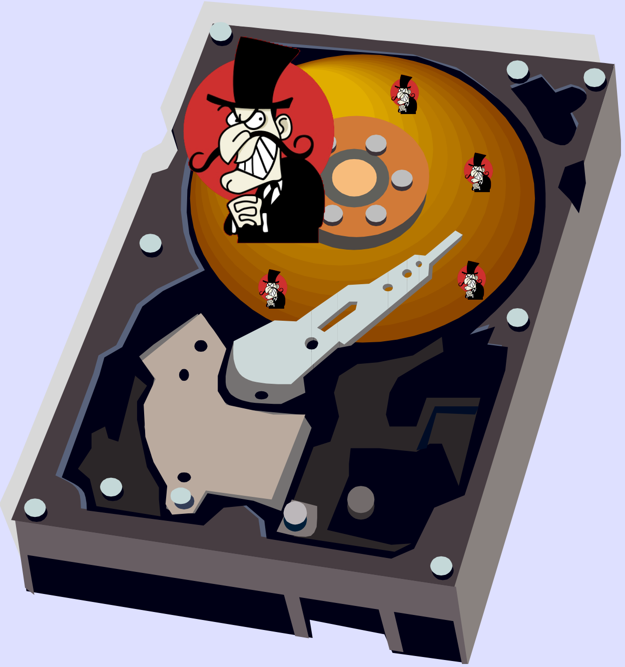
minimalize the impact of incident

- recover in proper manner
- not to be compromised again
- quickly ☺

compromised system

any file on the system is suspicious

- you may be able to remove a malware
- there could be another malware that you could not detect



wipe

don’t use files in the compromised system

- programs, documents, images

clean up the storage in the system

- HDD, SSD, flash memory

off-topic though

wipe to give away

data is still there even if formatted

- you can read it by special tools
- an electric microscope can read more
- causes leakage of secret data

you need to make sure data erased

```
# dd if=/dev/urandom of=/dev/<disk> bs=16M
```

recover

‘clean install’ from a scratch

- format the disk, use a proper OS image

apply OS patches to be up-to-date

- it could be vulnerable before patched
- update on secure network, behind NAT

install needed applications

- check upgrades, of course

recover(cont.)

disable unnecessary services

- the same as hardening procedure

check configurations

- if any weakness

change all password on the system

- any password might be stolen

replace

you may replace the compromised system

- spare server
- spare client

may want to secure the compromised system for further investigation

replace(cont.)

hardening the system

- update everything
- disable unnecessary services

check configurations

- if any weakness

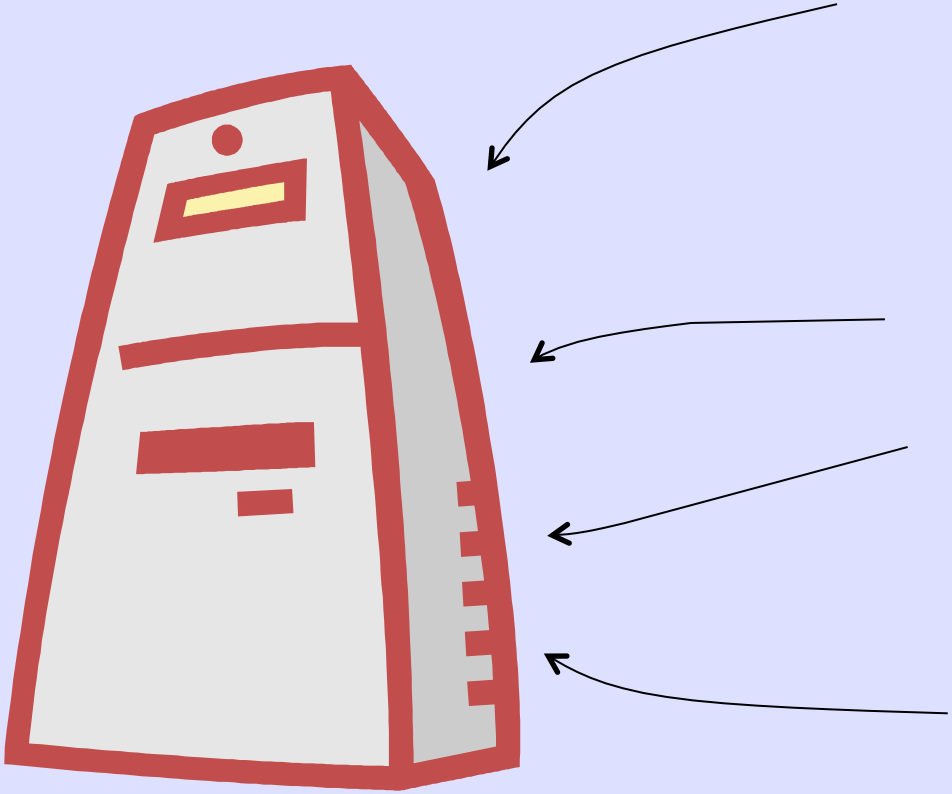
change all password on the system

- any password might be stolen

plan of archives

generations of backups

- configurations
- data files
- source codes



generations

you have a ‘good’ version of backup there

- if a system is compromised, malware might be also backup in the archive, you won’t want to restore that though
- if something goes wrong by change, you may restore the previous version

find a ‘good’ version from your archives

off-site Archives

2011 Tohoku earthquake and tsunami

- flushed buildings, data centers
- 4 local governments lost whole data on the family registration system

They have off-site backups ☺

- took about 1 month to recover though
- wanted to make sure nothing is missed

plan of remote fallback

difficulties to recover locally

- no hardware available
- long-term power outage
- fire, disaster

you can restart your service, if resources available somewhere

- flexible

points to consider

DNS

protection

- the same (or similar) level of protection
- update ACLs, keys if needed

service relationship

- check other systems if they need to update ACLs on their side