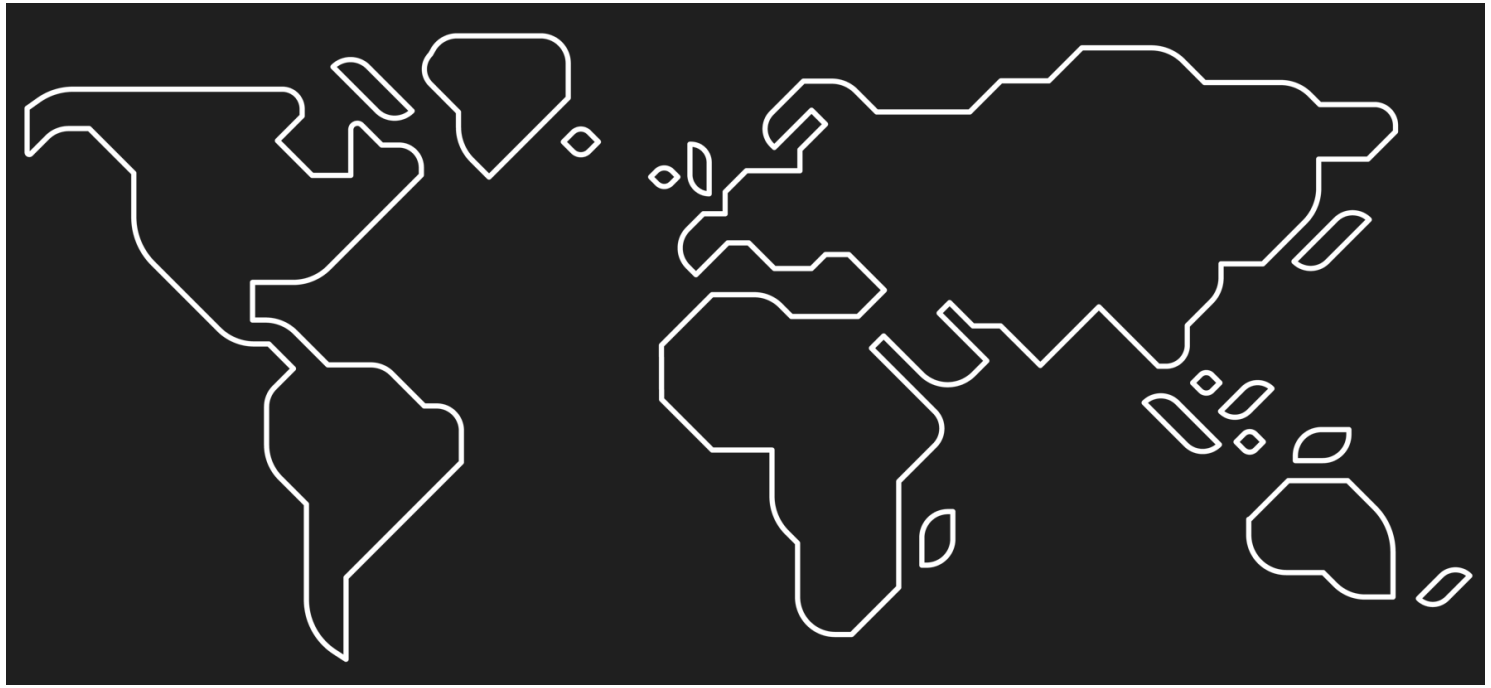
Hydro

Cyber attack 2019 Hydro ASA

Peter Uhrenholt

Magnor 2024

Norsk Hydro ASA



- 40 countries
- 140 locations
- 33.000 employees around the world
- Result of 2,4 billion NOK

Norsk Hy

the world

Preparation for a potential cyber attack

- Restrictions on what to download and how
- Restrictions on web sites and links
- Firewall established
- Behavior training

- Contingency plan in place for years
  - IT breakdown
  - Local cyber attack
- Backup to external servers
- Backup to IBM servers


Tønder Handel & Transport
ABTEK International | Uffe Nielsens...
Hydrovej
Fabriksvej
Ribe Landevej
Møblér med ndbo Center
Furniture store
Stressless
Furniture store
Hydro Precision Tubing Tønder
Tønder Vandværk
Hydro Extrusion Denmark A/S
Bygmestervej
Skovænget
Karl Otto Pilgaard
Tønder Genbrugsplads
Malervej
Skriver A/S
Snedkervej
Super Dæk Service
Auto repair shop
Tønder
Søren Johannsens

The attack!

Seen from Hydro Extrusion Denmark A/S

- Monday March 18th 2019 at 23.00 the first report came to local IT.
- Shortly after second plant in Denmark reported issues.

- Within the first hours it was clear that a central serv
  Norway had been encrypted and ransom was d
- Local management was alerted, and ev
  closed and dis-connected.

- Escalation to IBM
  - Austria, Polan and Denmark effected

- First meetin March 19th at 08.30
  - Conti
  - stomers?
  - the employees?
  - big is the problem?
  - Which systems are affected?

Everything was documented!


English

19.03.2019

[March 19, 07:00 CET] Cyber attack against Hydro

All Hydro employees: Due to a cyber-attack against Hydro, employees must NOT turn on their Hydro PC's. Phones are ok to use. We will update as soon as we know more. This is not a drill.

Immediate problems

Can we produce?

- Packing list
- Production orders
- Die storage
- CNC programs
- Drawings

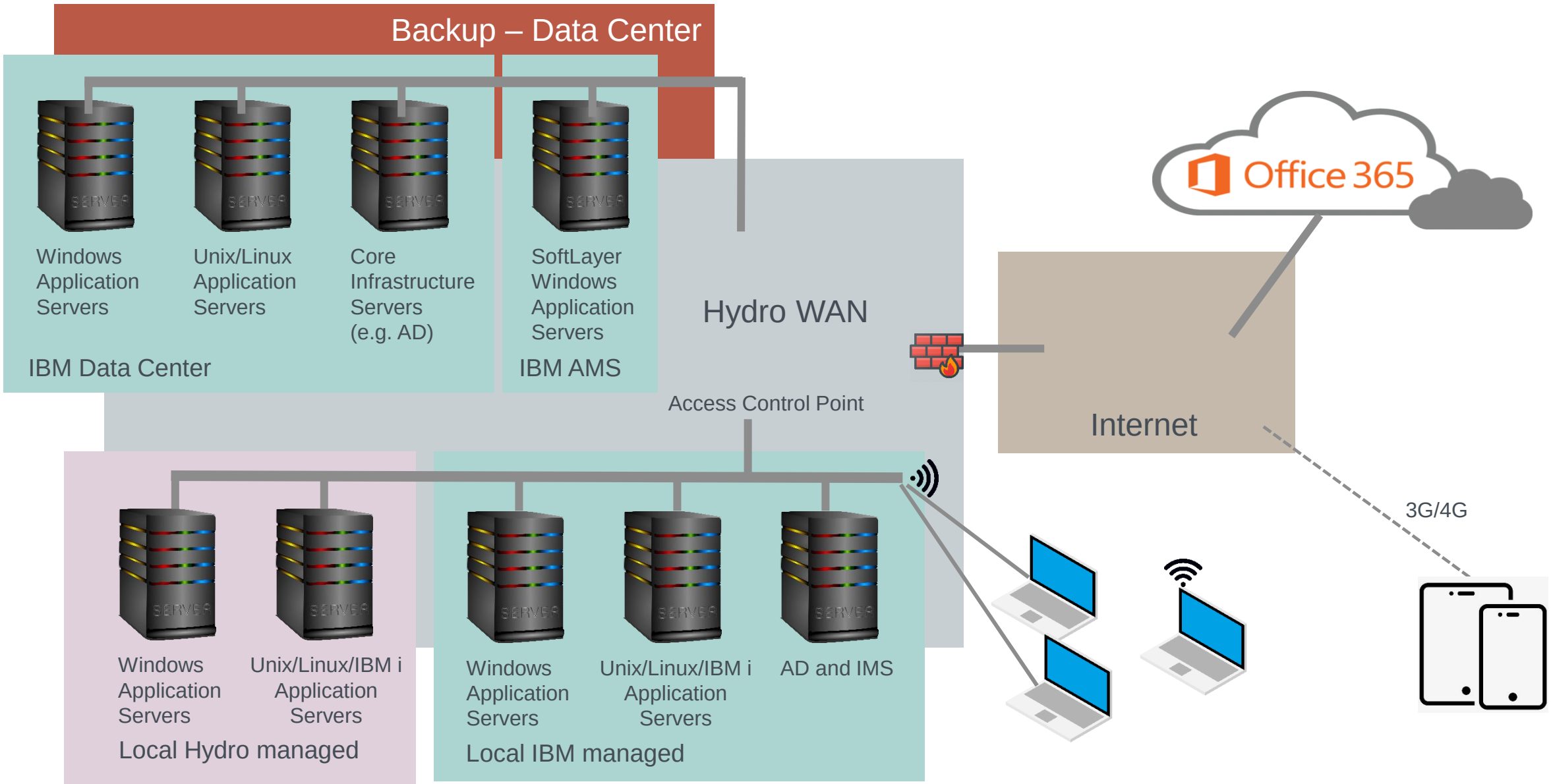
- Expected **full** stop: 3-5 days

- Next meeting at 12.00

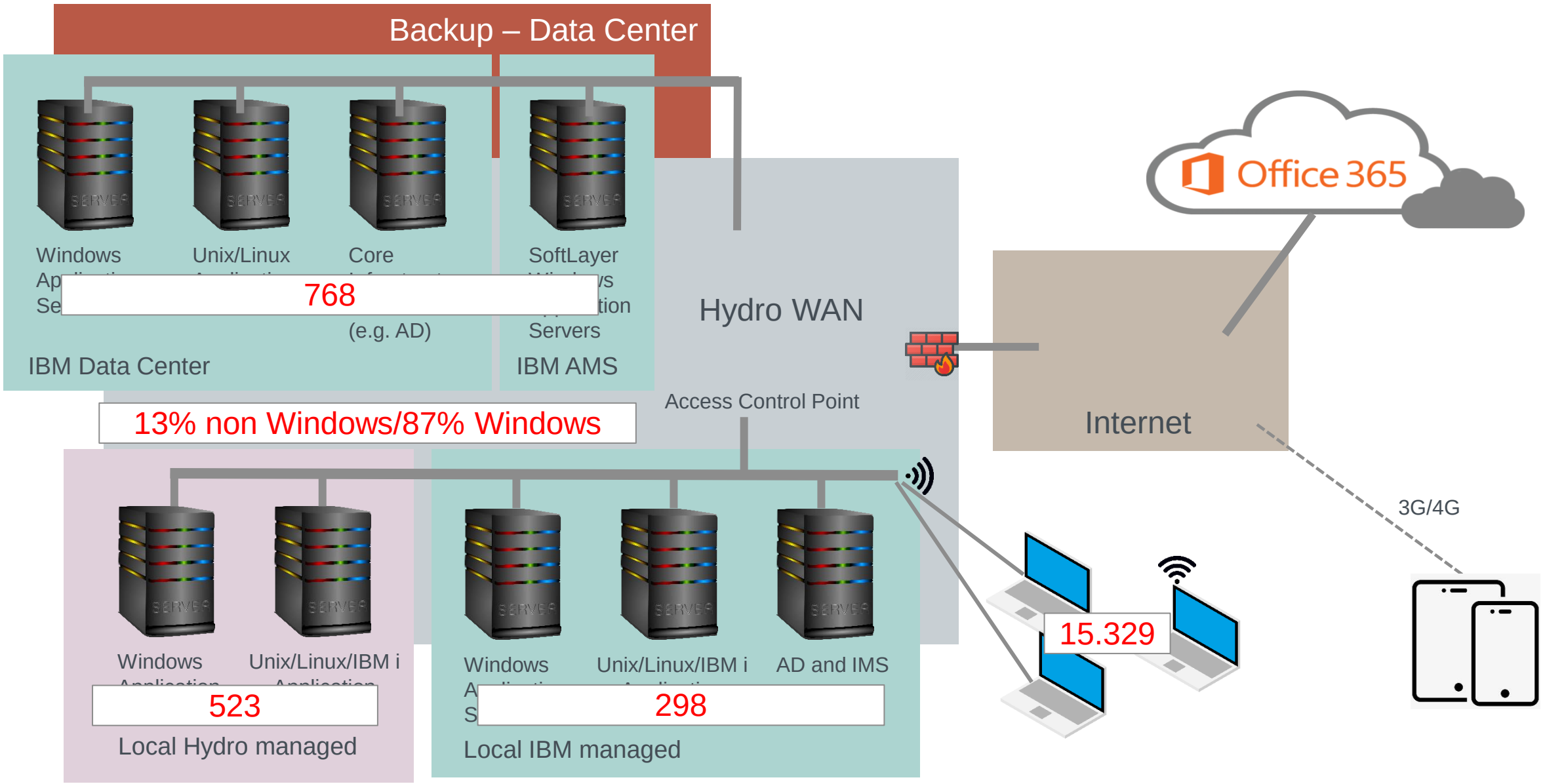
The film about the cyber attack

- https://www.youtube.com/watch?v=S-ZlVuM0we0

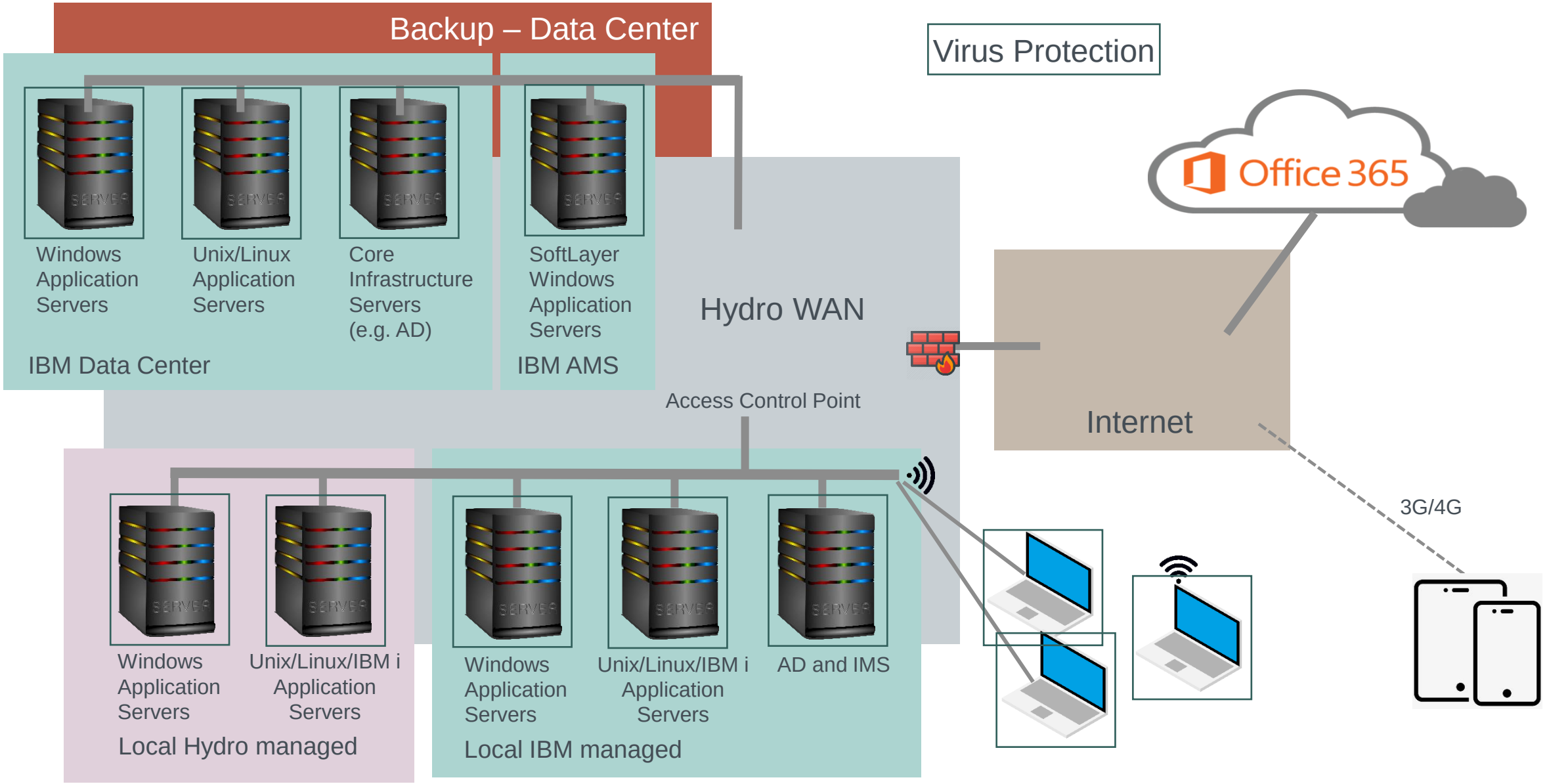
Extruded Solutions IT Infrastructure (simplified)



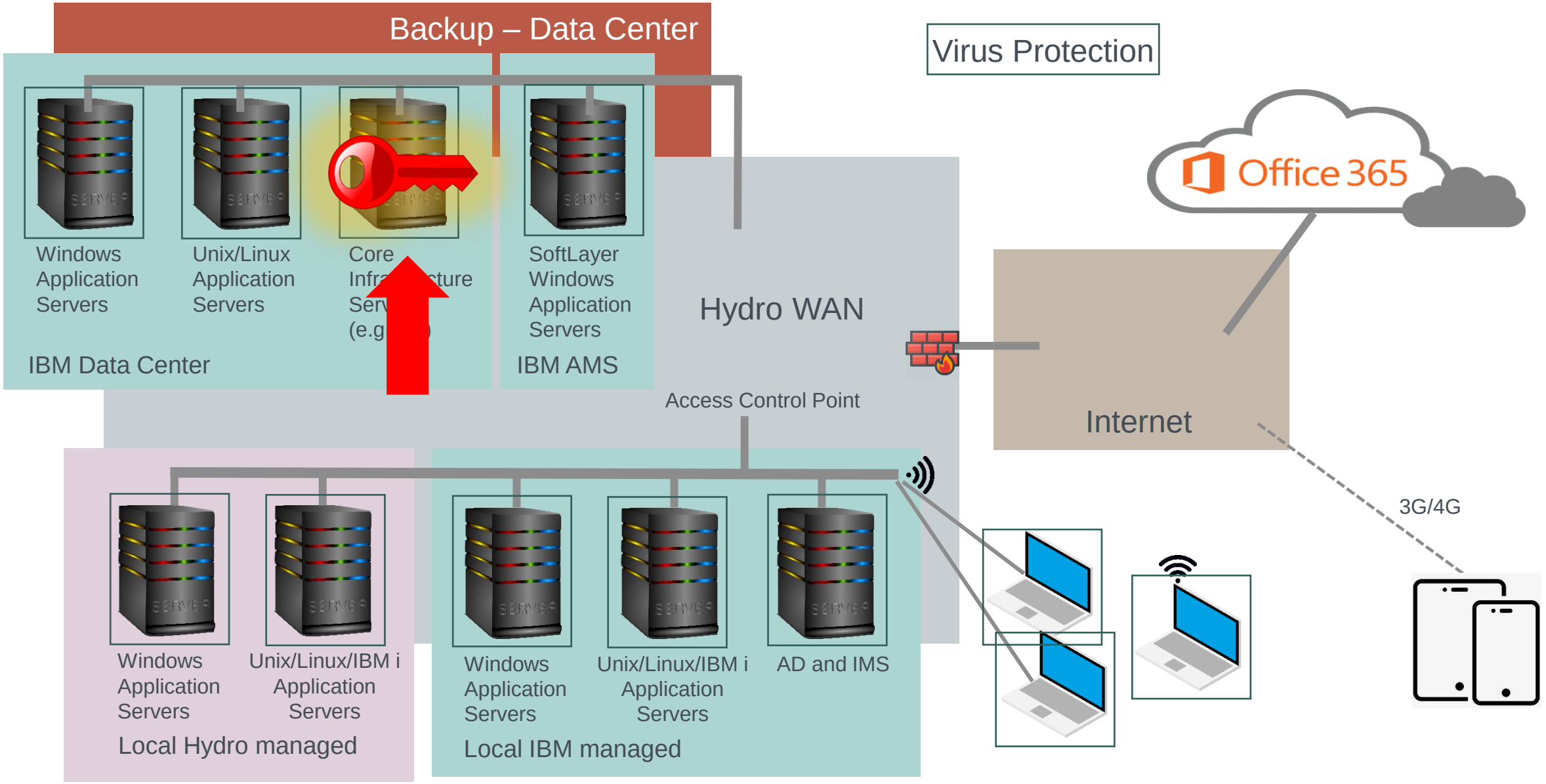
Extruded Solutions IT Infrastructure (simplified)



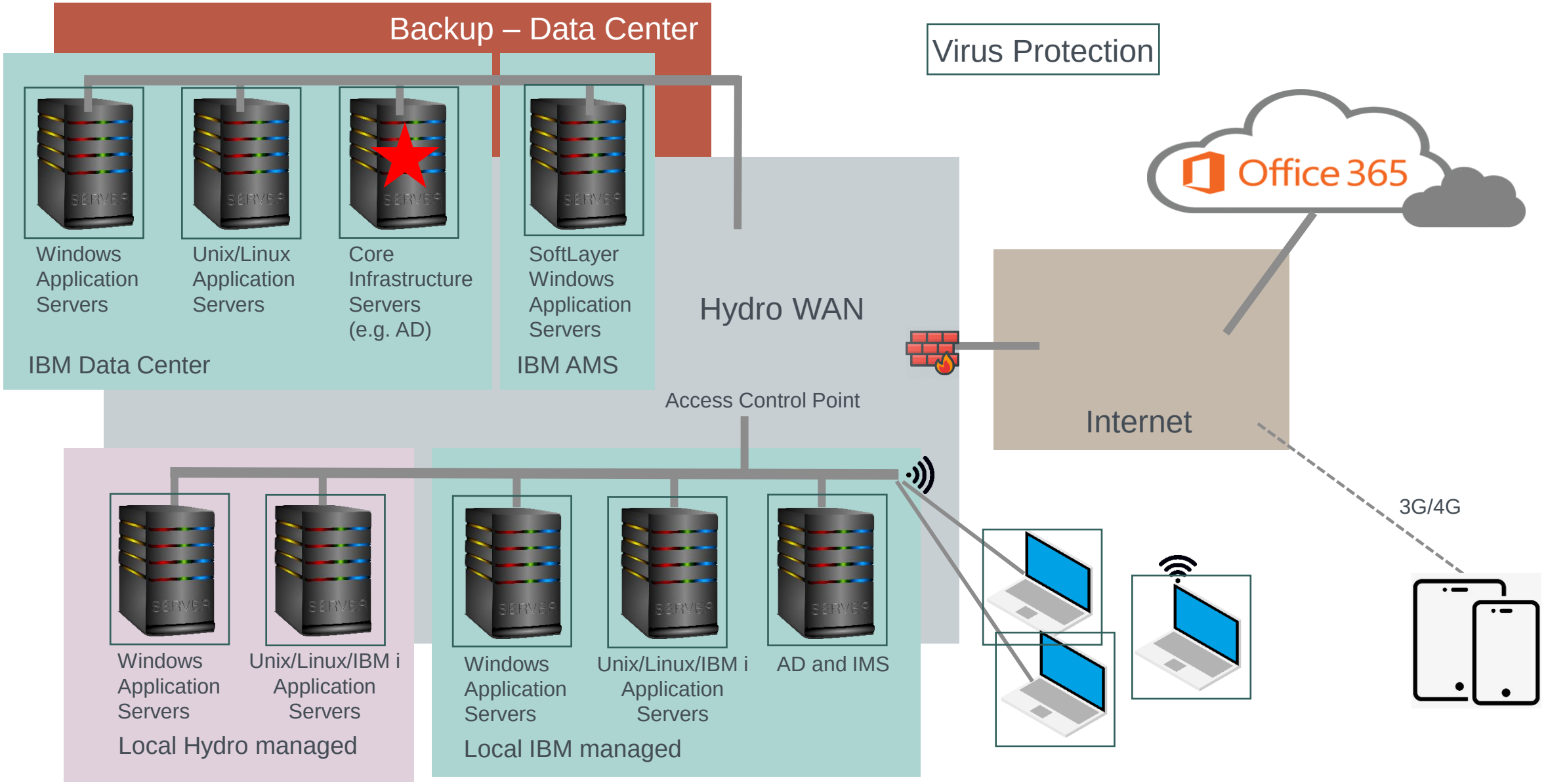
Status before Feburary 2019



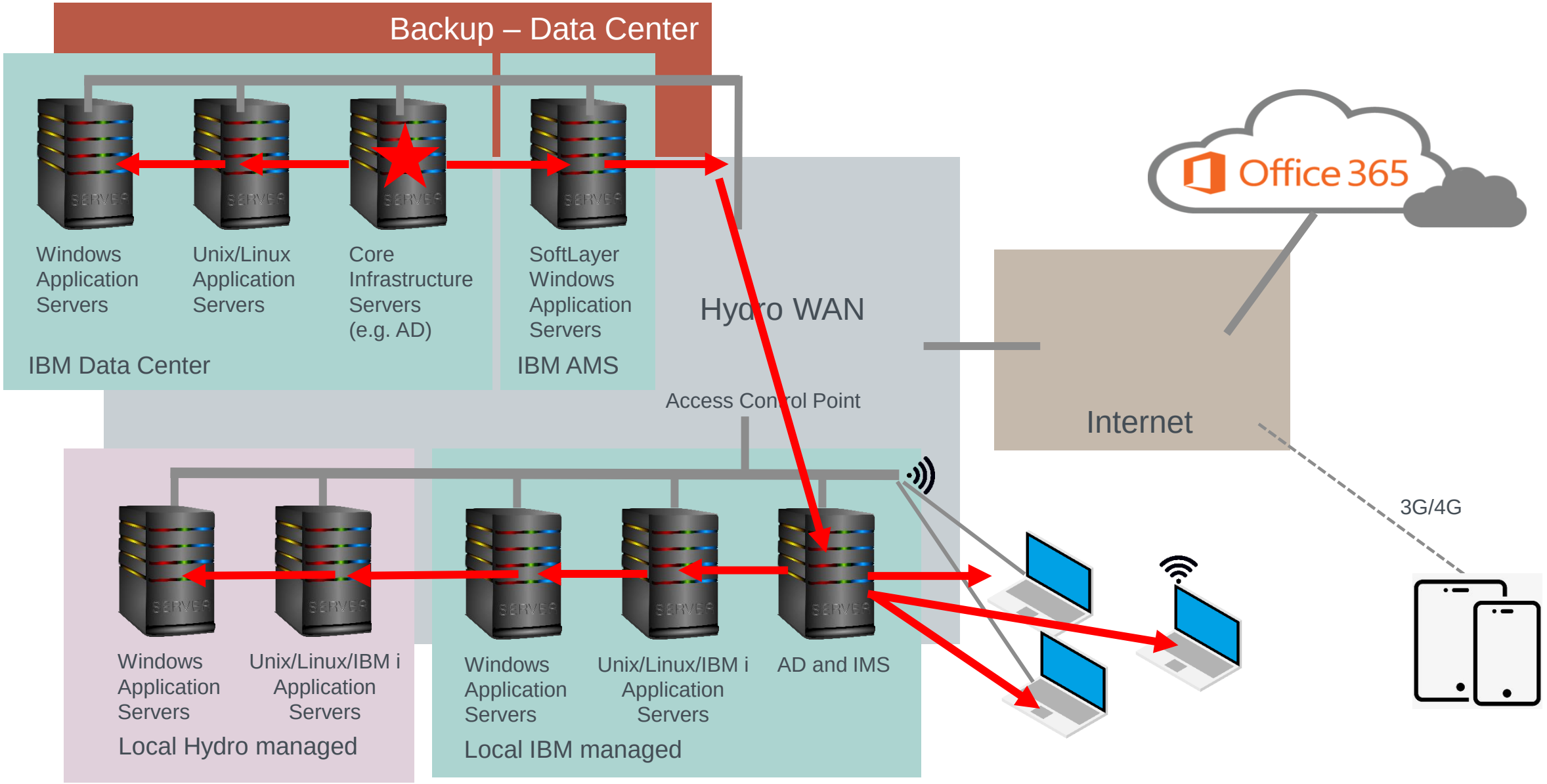
Start of attack in Feburay 2019



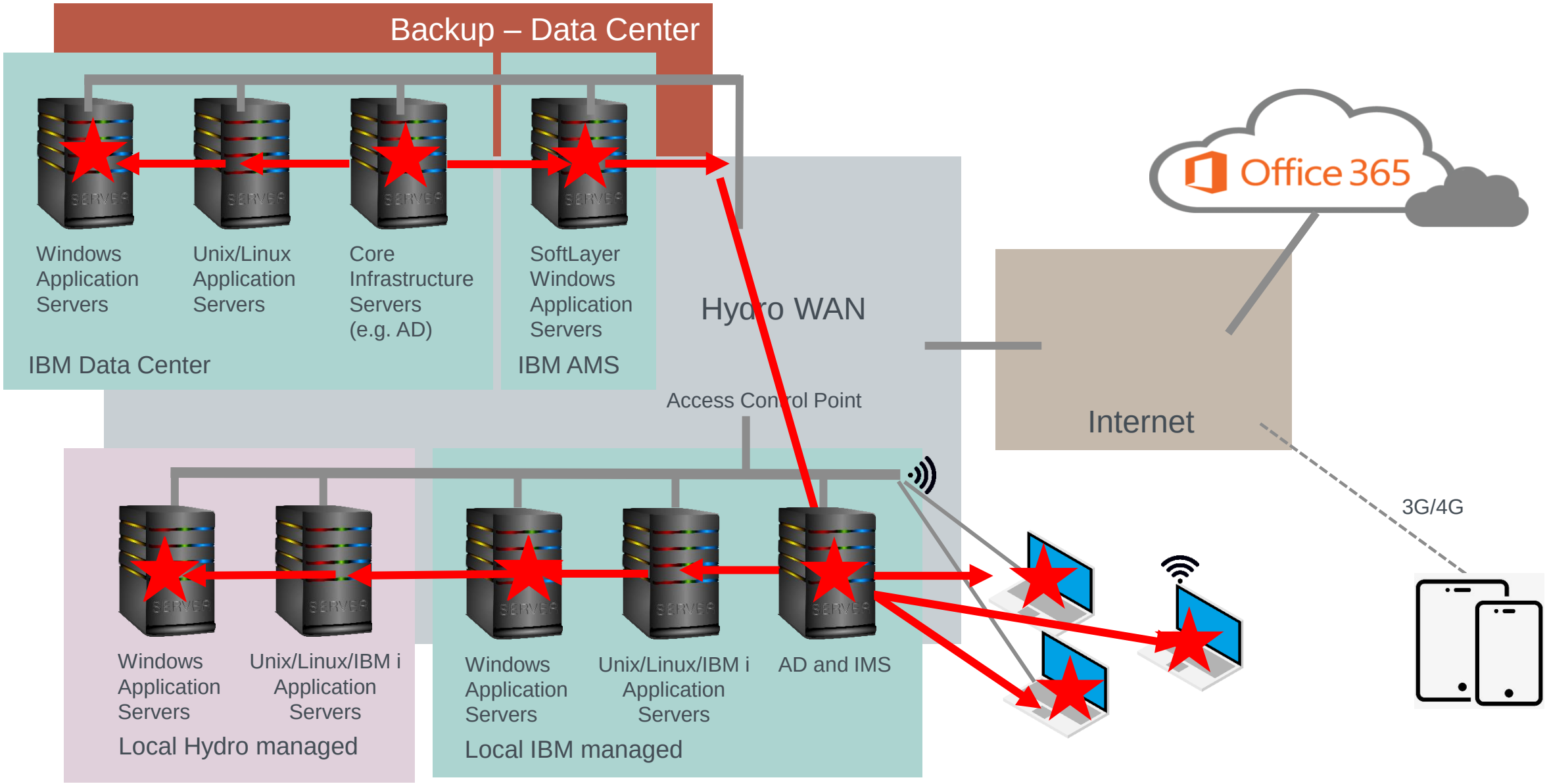
Start of attack in Feburay 2019



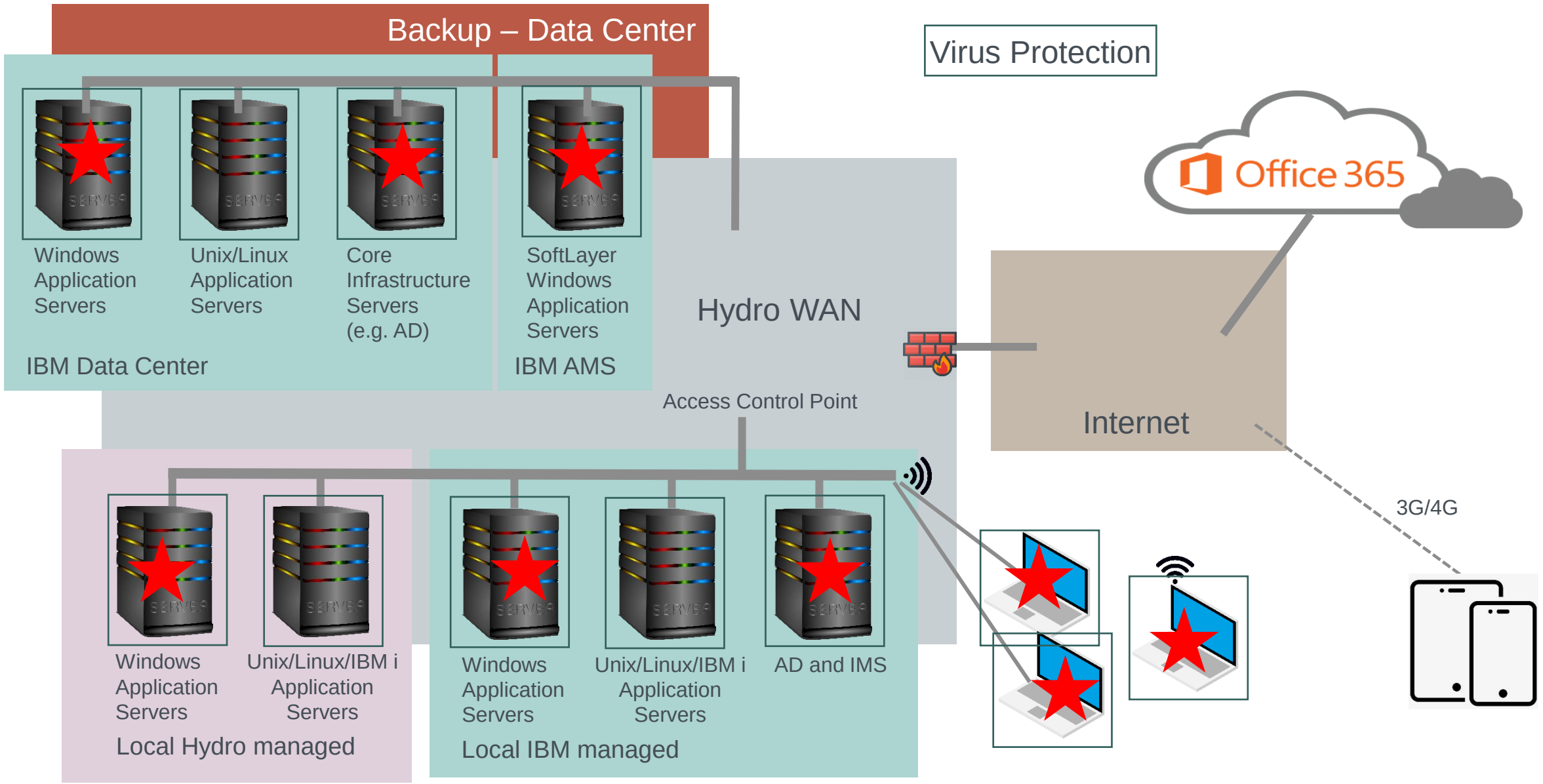
Start of attack in Feburay 2019



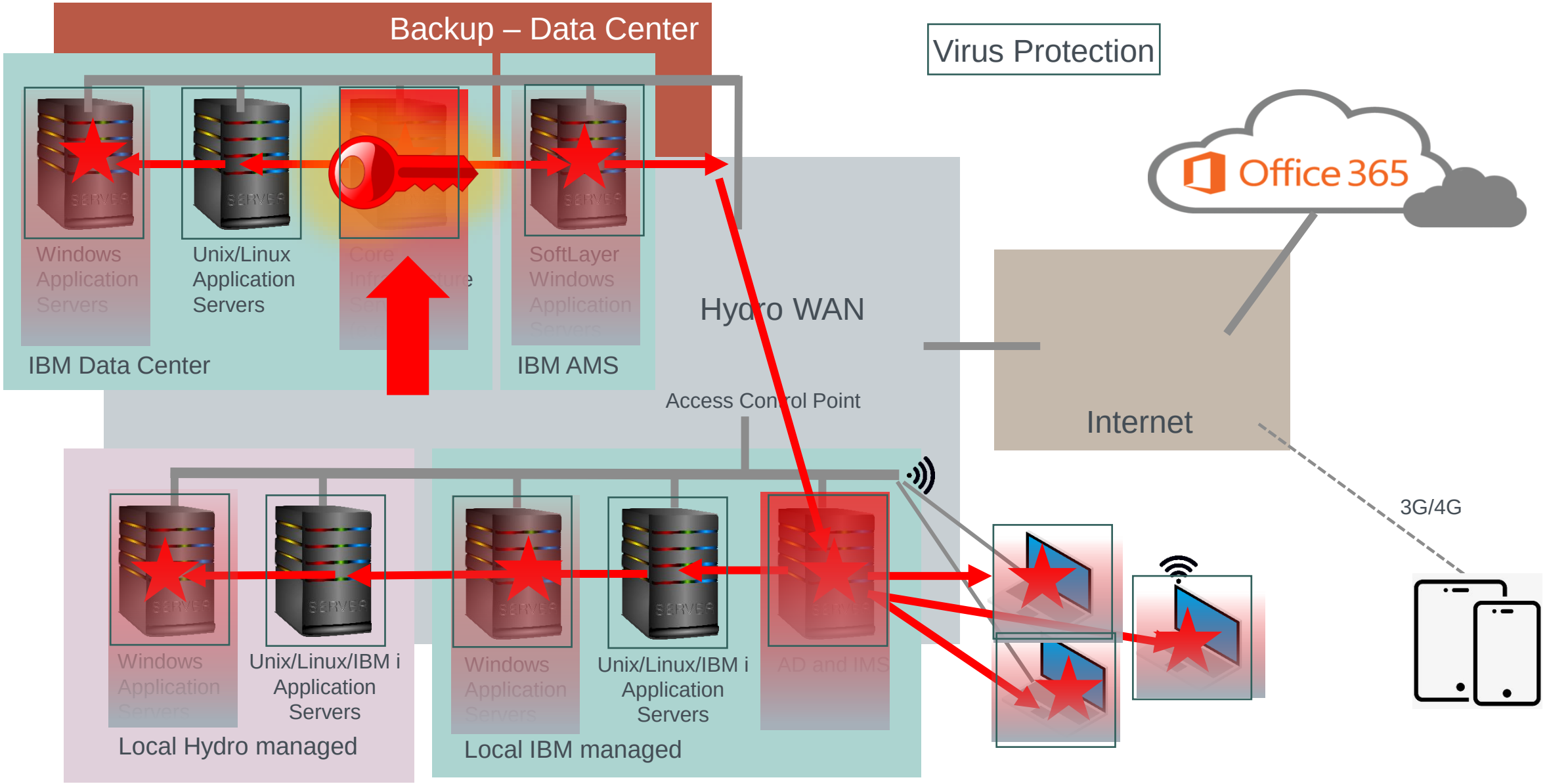
Start of attack in Feburay 2019



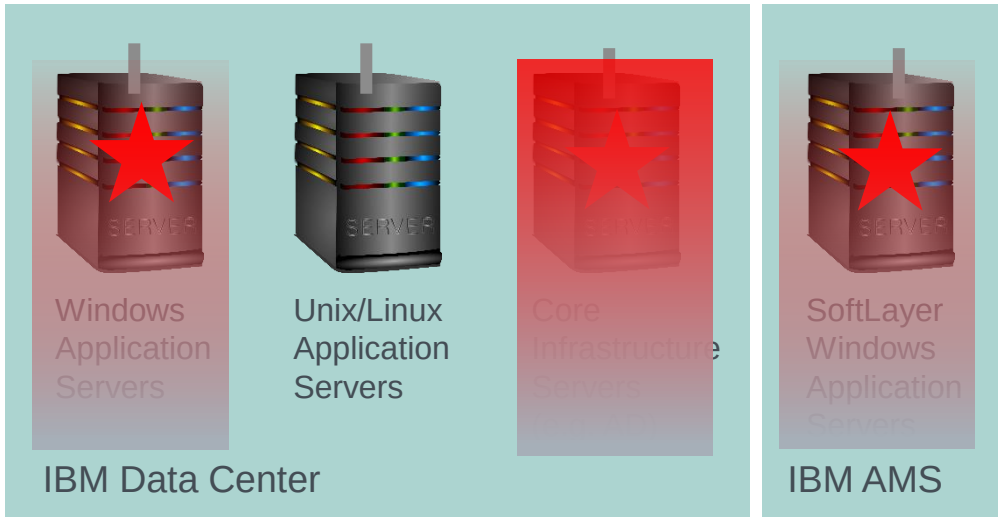
Status before March 18, 2019

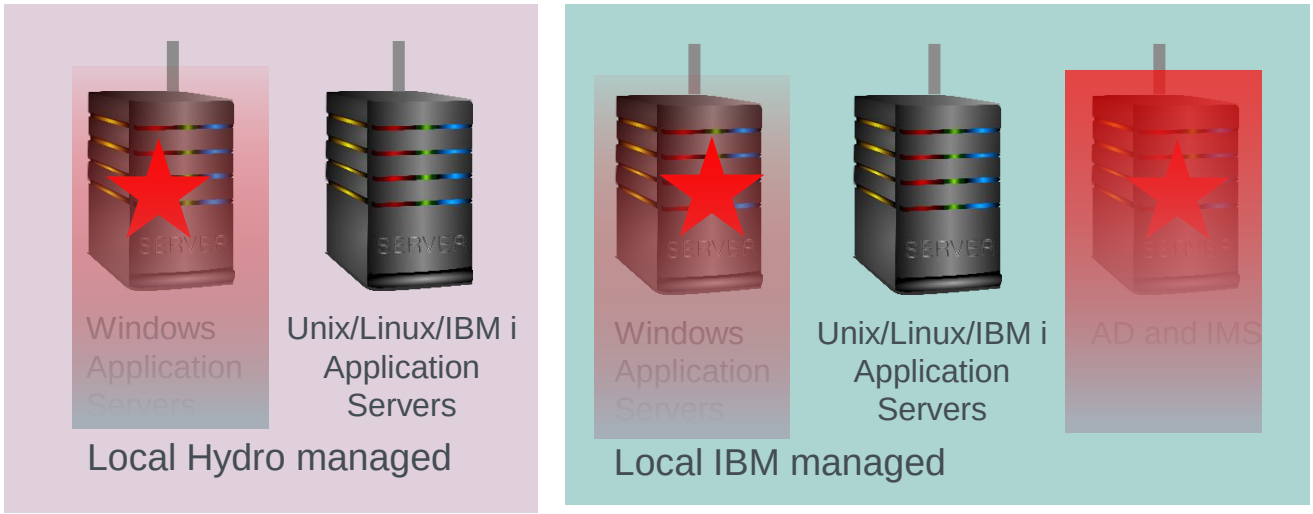


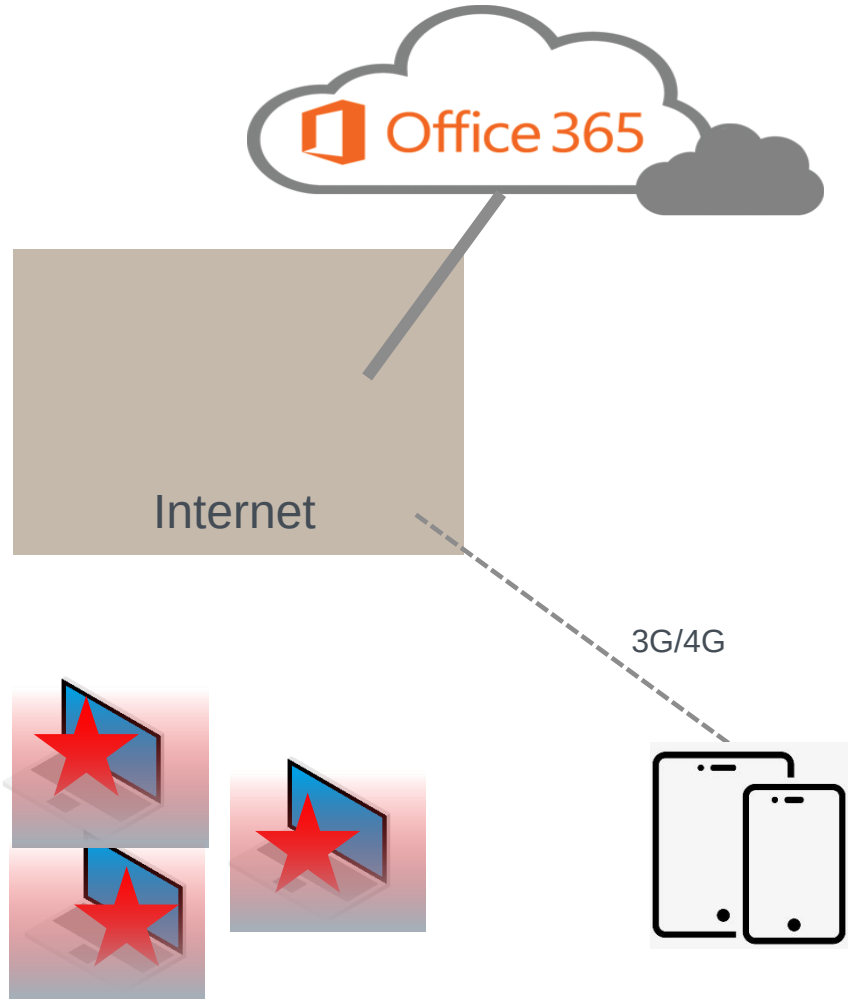
Trigger on March 18/19, 2019



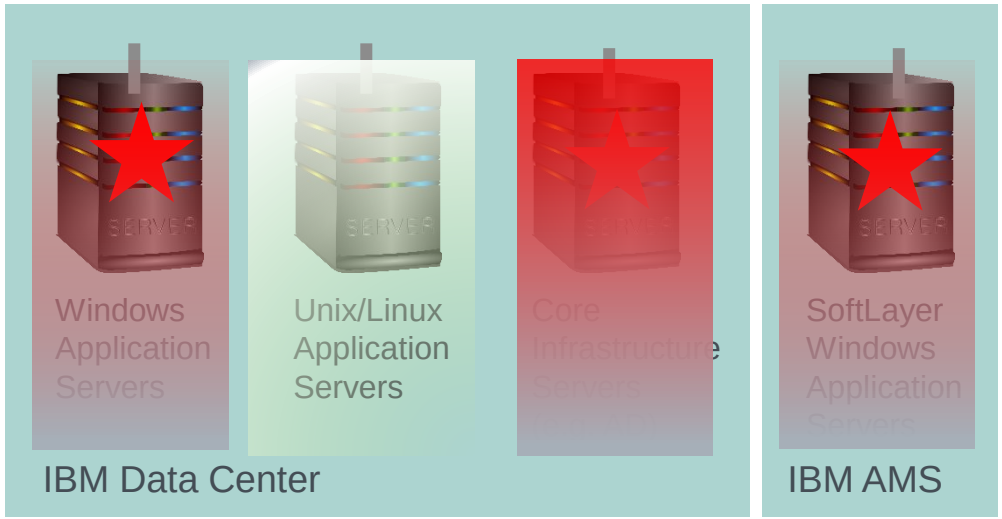
Shutdown of all connections and servers on March 19

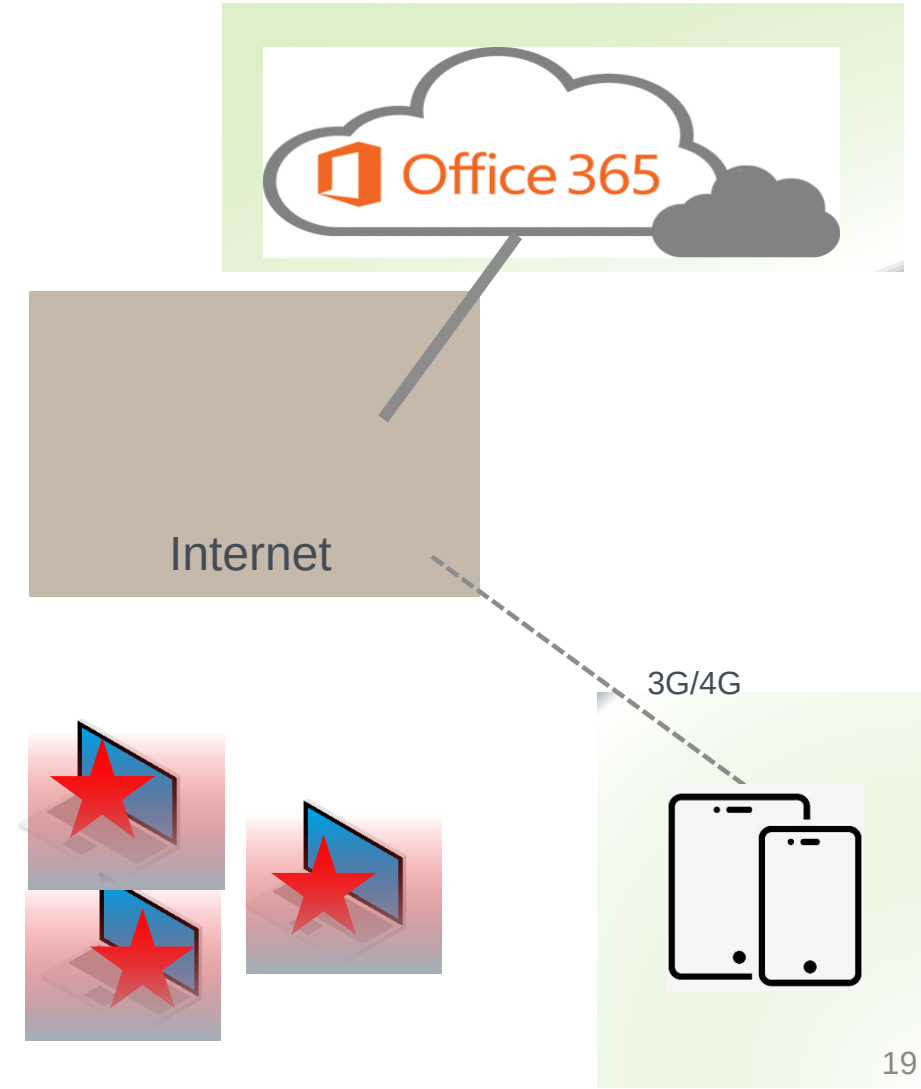


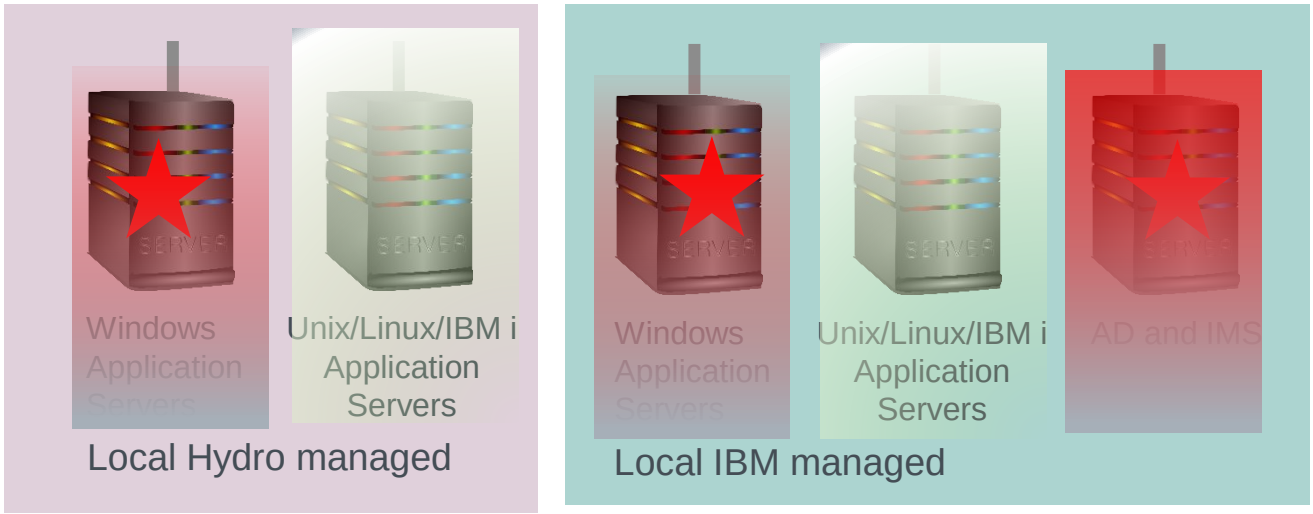




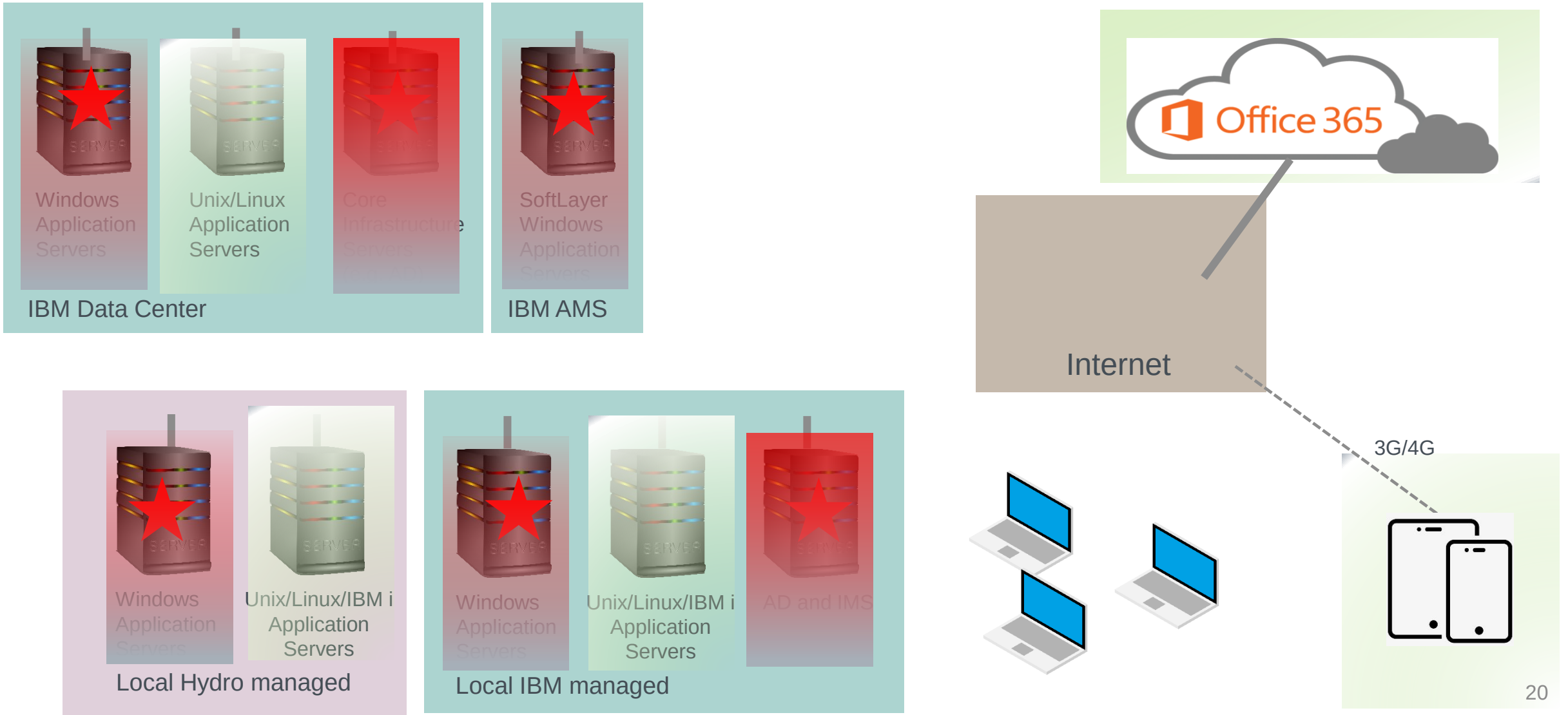
Shutdown of all connections and servers on March 19







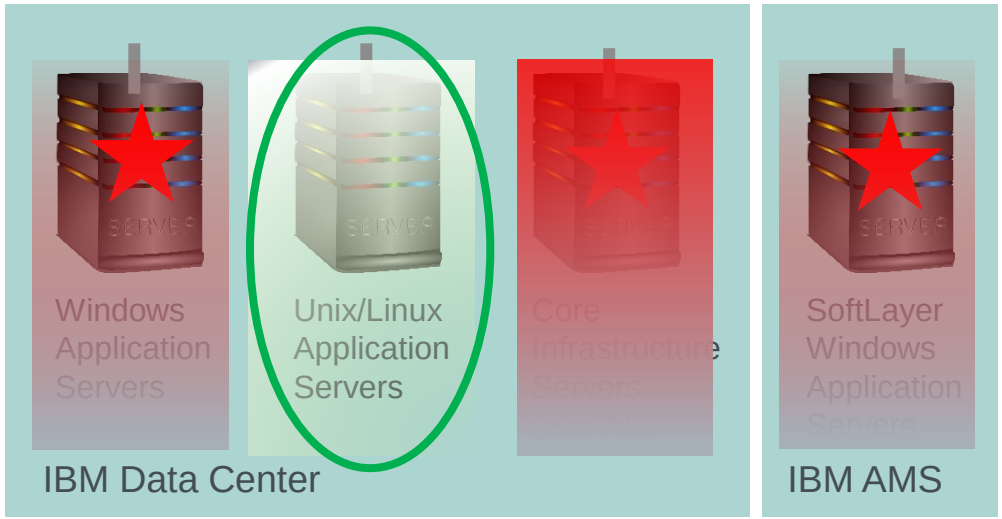
Recovery process since Mach 20

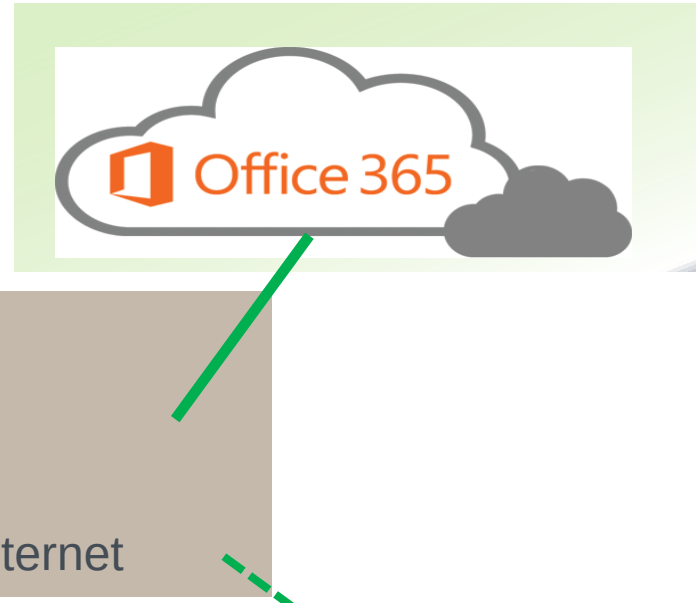


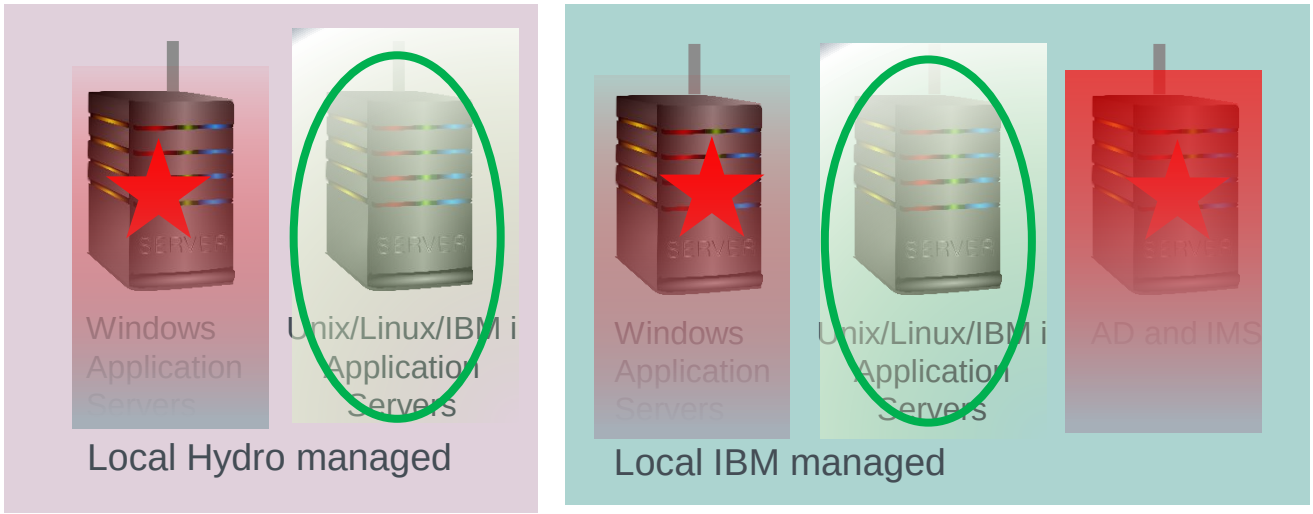
Recovery process since Mach 20

Hydro

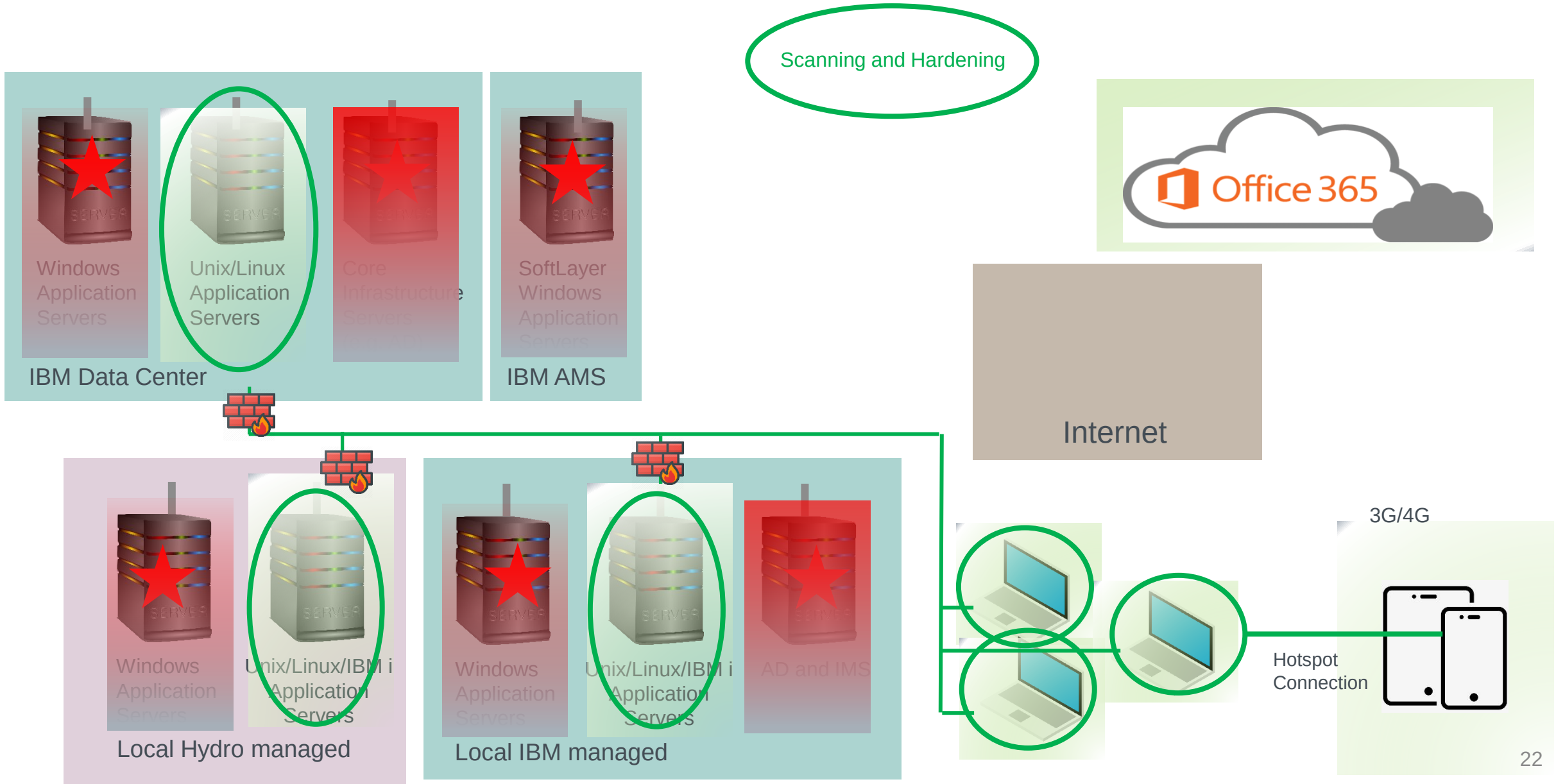
Scanning and Hardening



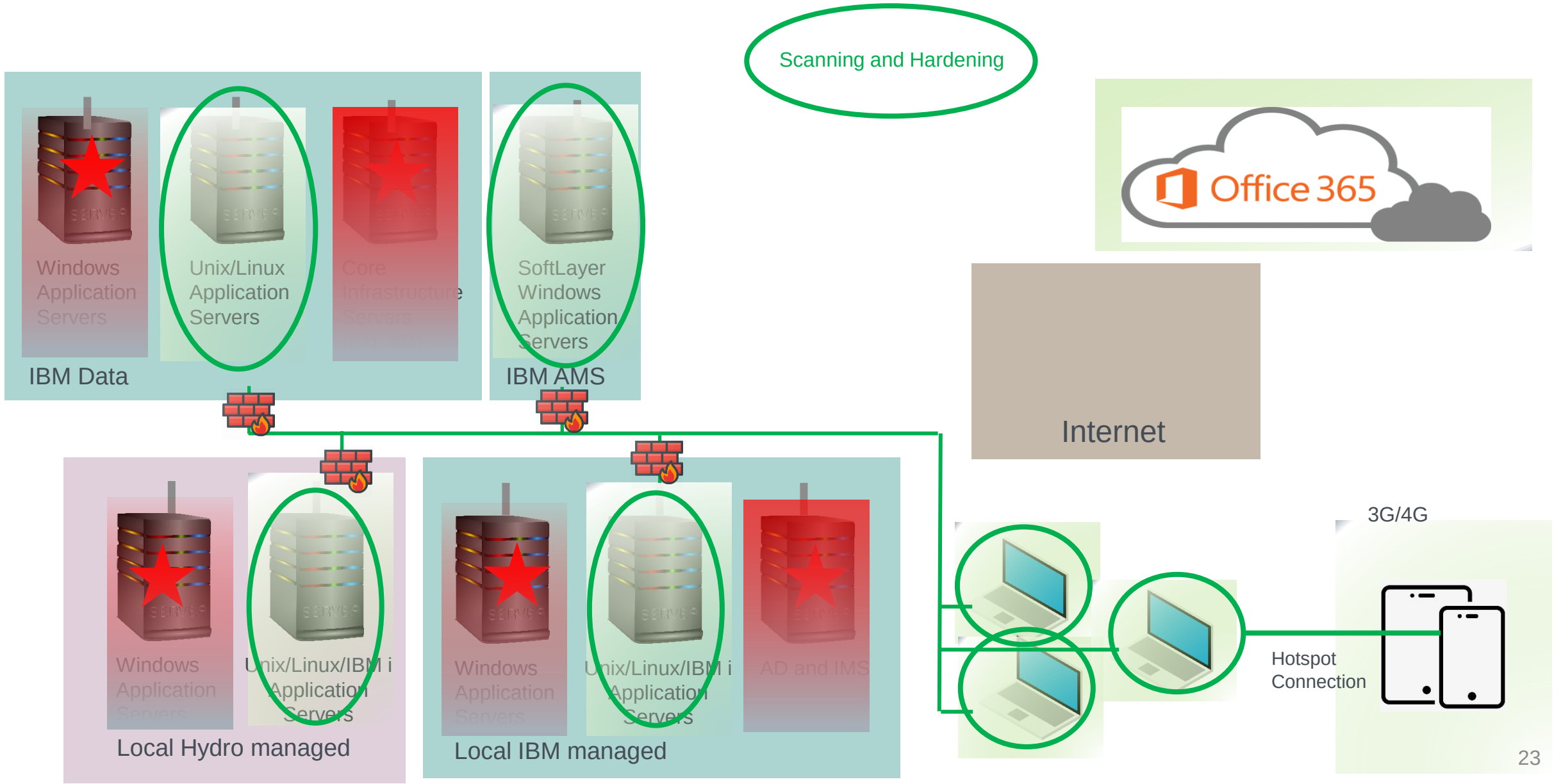




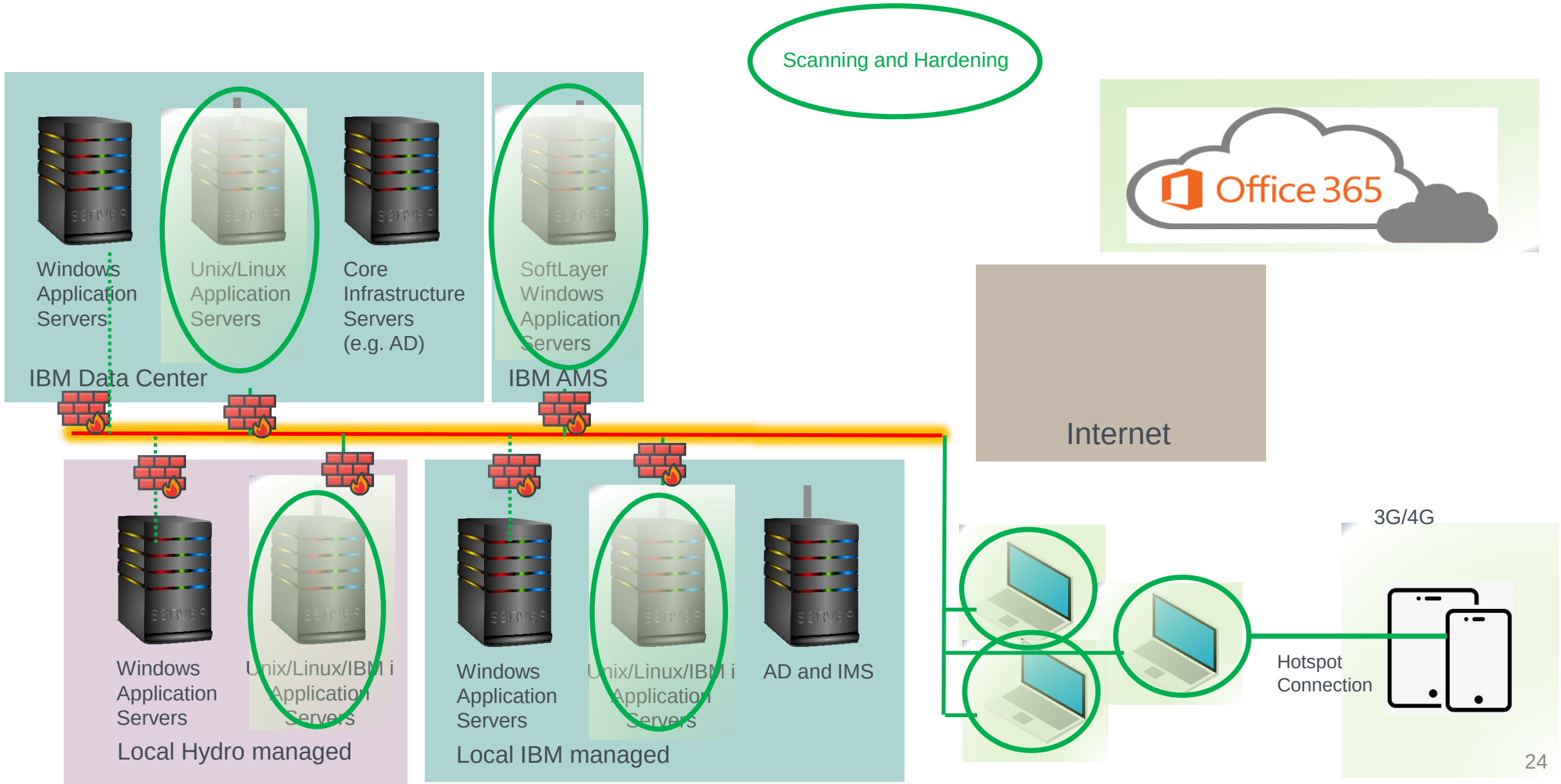
Recovery process since Mach 20



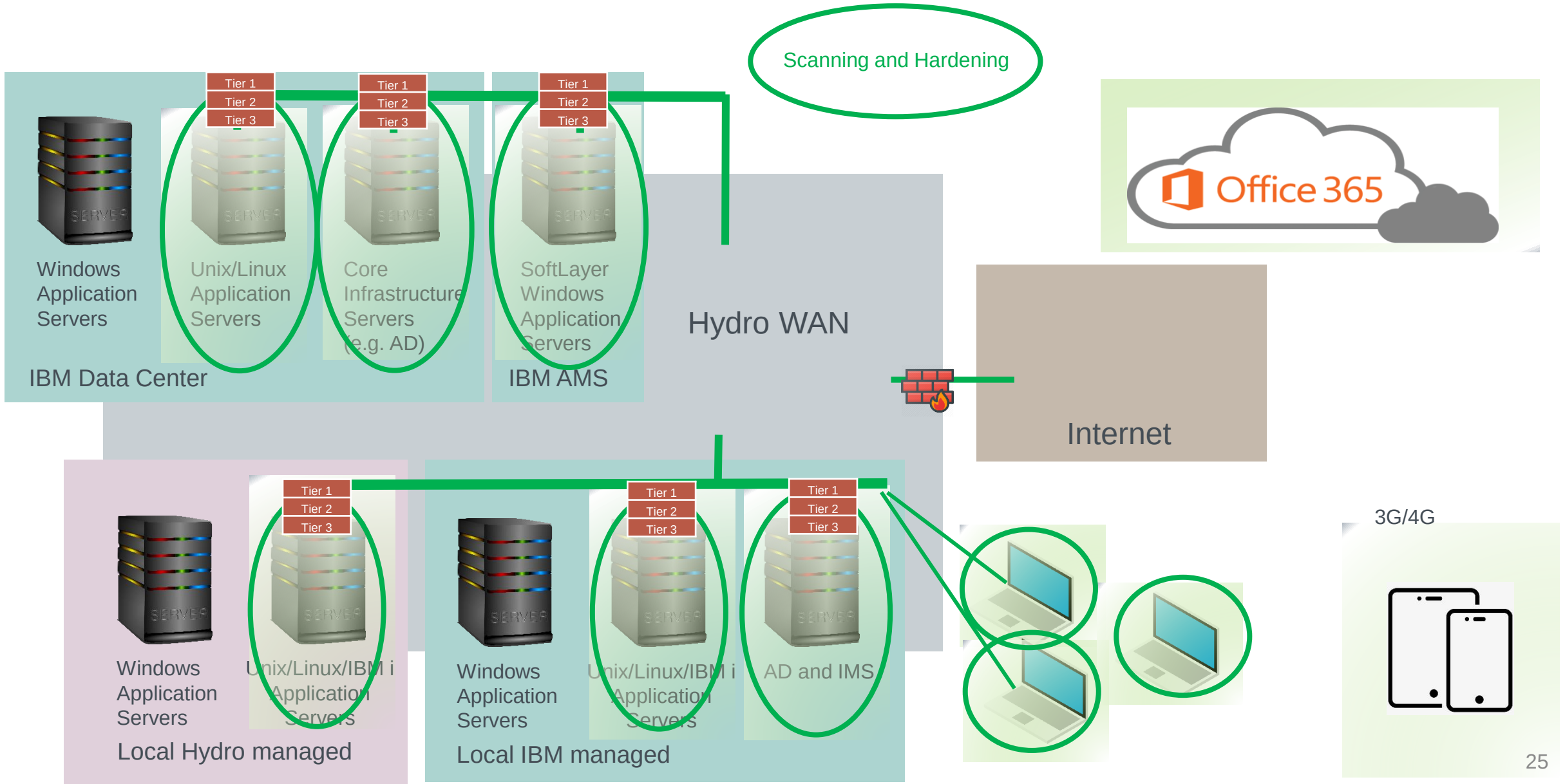
Access to non infected systems



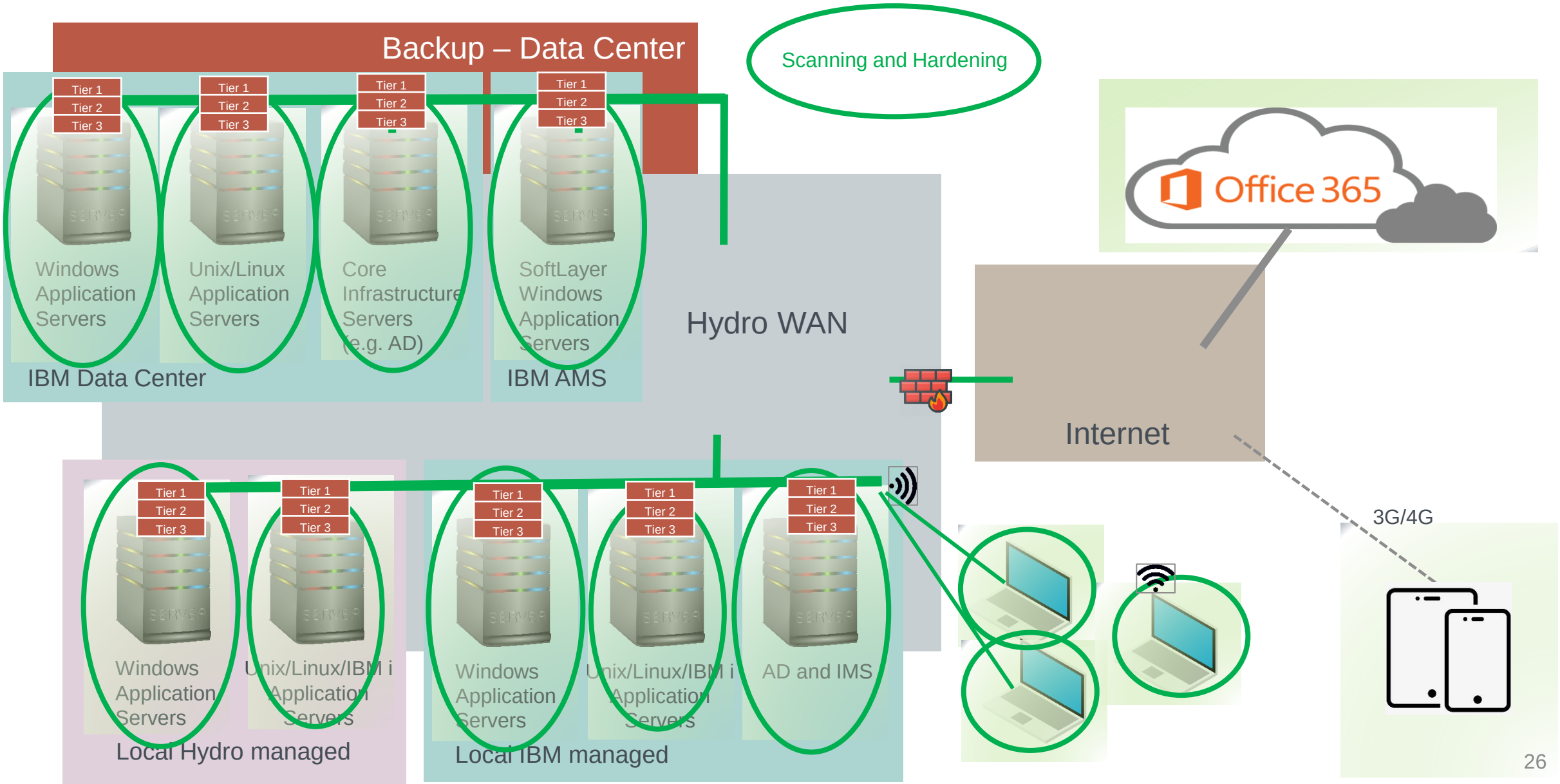
Access to non infected systems



Rebuilding network functionality



Final recovery



Local issues

- Lost access to orders, production planning and invoicing.
- The very old DOS based ERP system used in a few plants was not infected
- Die storage robot can work, but overview is gone (15.000 dies!)
- Profile dimension measurement is working off-line
- Capability calculations can be done manually
- Mechanical testing can be done off-line
- No access to profile drawings.
- Communication was down through PC and web site.
- Facebook was used to update Norwegian colleagues.

- Establishing local network
- Should we go for LINUX/Ubuntu solutions?
- PC’s can be switched on – OFF-LINE at 14.00

Discoveries within the first days

- IBM backup of die storage system did not exist!
- A colleague had downloaded all die drawings few weeks before.

- Real production of profiles started 26 hours after the attack
  - Based on experienced operators
  - Based on verbal production orders from customers
  - Fully manually controlled processes and calculations

- Test machines were re-programmed internally

- The attack happened in Norway ⟶ Norwegian cyber police was involved and initiated their investigation.
- The virus had been placed as a sleeping virus weeks before the actual attack!
- Probably through a USB stick!
- Several backups were infected!

- Colleagues who could not do normal work assisted in challenging production areas.
  - HSE issues?

Challenges and considerations

- SAP finance was down for weeks and monthly/quarterly report to Hydro was delayed.
- Can we get process data directly from PLC’s?
- Are we able to calculate process variation manually (SPC)?
  - Release of productions?
- How to register who is working?
- Does anyone have IT skills to support IT?
- Perimeter safety?
- How to communicate with banks, tax etc?

- Mental health challenges
- Long working days
- Cancel all non-critical meetings!
- Does the pay role system work?
- Free lunch for all!
- The communication with customers got tougher after 10 days!
- Daily update from HQ
- Competitors started to mis-inform customers.

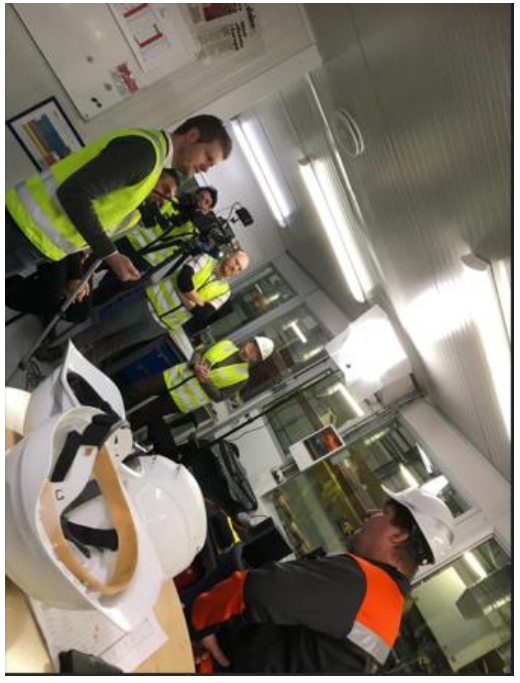
New/changed processes

- NO visible passwords in production areas!
- Cyber security awareness training
- Regular test of IT awareness
- USB stick drop test
- Lock your screen

- Daily meetings ended May 21st after 9 weeks!

How to let others know what had happened?

- From the very beginning, Hydro chose to very open about the attack.
- Daily press conferences about the situation were performed from HQ.
- Major interest from the media – BBC, Microsoft, Dagens Næringsliv and other.



Openness

Hydro was awarded Åpenhetsprisen 20.09.2019 because we dared to be open about the cyber attack

Fra.v Inger Sethov, Eivind Kallevik og Egil Hogna fraHydrounder en pressekonferanse om cyberangrepet på Hydro. (.Foto: Vidar Ruud / NTB scanpix)

Hydro får Åpenhetsprisen: Turte å være åpne da de ble utsatt for massivt dataangrep

en omfattande cyberattack mot koncernens IT-system. Nu pressas de på pengar av angriparna.

Bloomberg

Hydro

Industries that matter