bcs The Chartered Institute for IT

Information Risk Management and Assurance Specialist Group

kuppingercole ANALYSTS

WELCOME TO THE WEBINAR

Cyber Resilience – Backup or Else

Mike Small

Senior Analyst | KuppingerCole

Hybrid Multi-Cloud IT

Enables digital transformation but introduces new risks

CISO Important Trends

KuppingerCole Cyber Security Council held in Berlin in May 2022 identified 4 key areas

The KuppingerCole Cybersecurity Council brings together information security professionals in leading positions from across many industries.

1 **Cyber Resilience**

How your organization can manage when IT resources are compromised.

2 **Cyber Hygiene**

This lays the foundation for all other cyber security measures.

3 **Cyber Insurance**

This needs to cover the whole business risk. How can you rebuild the whole business not just IT

4 **Board Training**

In cyber security it is often missed where priority is given to reporting.

World-Class Information Security Experts | KuppingerCole

Digitalization Increases Cyber Risk

“Ransomware and threats against availability rank at the top during the reporting period.”

1 **Royal Mail**

Royal Mail hit by Russia-linked ransomware attack.

2 **MOVEit**

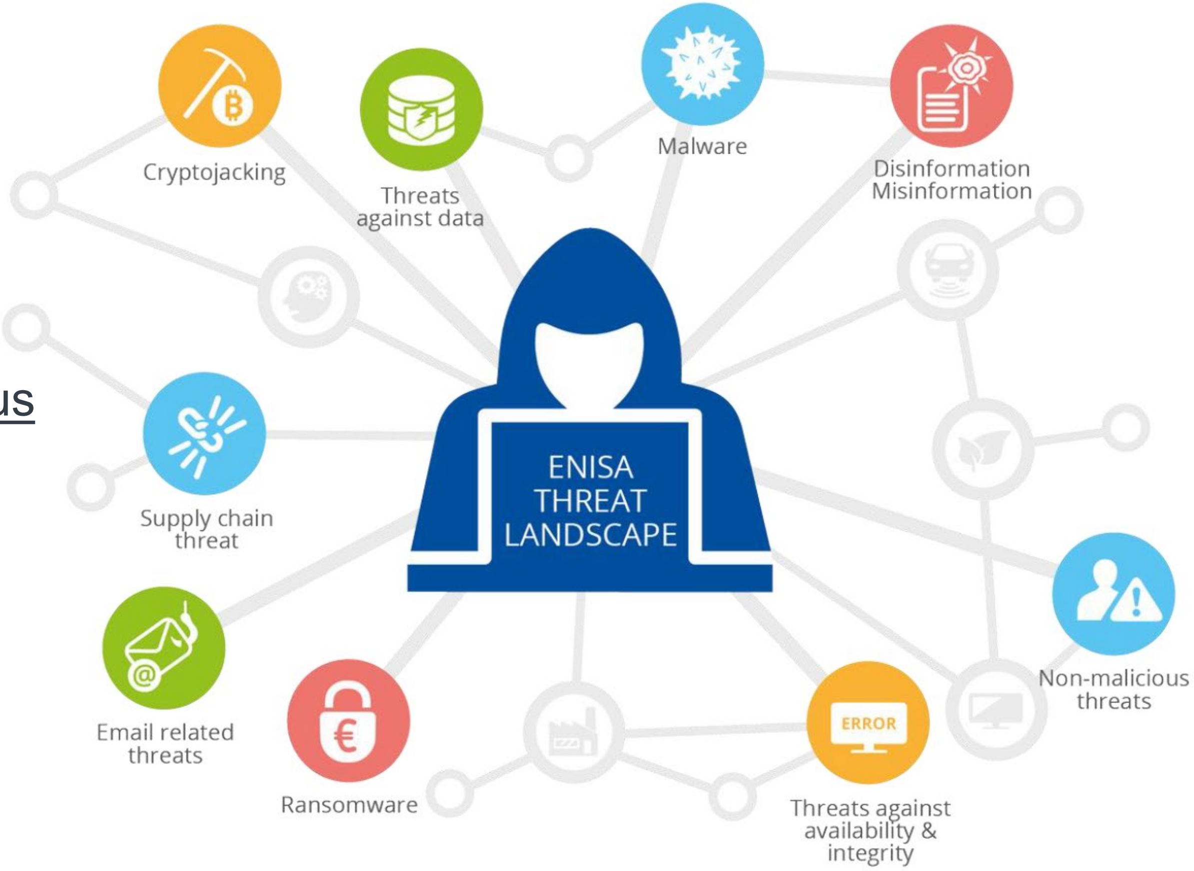
The BBC, British Airways, Boots and Aer Lingus are among organisations affected

3 **DoppelPaymer**

..cyber-attack on a hospital in Düsseldorf contributed to the death of a patient.

4 **More Organizations are at Risk**

And need to act now.



ENISA Report Threat Landscape 2022

The Need for Cyber Resilience

Governments around the world have introduced regulation to counter cyber threats

1. **US - Executive Order 14028**
   ..needs to make bold changes and significant investments in order to defend..

2. **EU - Directive (EU) 2016/1148**
   ..need to adopt a national strategy on the security of network and information systems..

3. **EU NIS 2**
   .. The digital transformation of society (..) has expanded the threat landscape..

4. **NIS 2 – holds the board responsible for cyber resilience.**

2. NIS 2 vs. NIS 1

NIS 2 extends the scope across more organizations and introduces more stringent measures.

NIS Directive (EU) 2016/1148 Overview

The UK Network and Information Systems Regulations (2018)

Affected Organizations

- Energy: electricity, oil and gas
- Transport: air, rail, water and road
- Banking: credit institutions
- Financial market infrastructures
- Health: healthcare settings
- Water: drinking water
- Digital infrastructure

Obligations

- Ensure security appropriate to the risk
- Prevent and minimise the impact of incidents affecting digital services
- Take account of the DSP Regulation

Establish Policies

- Risk analysis
- Human resources
- Security of operations
- Security architecture
- Secure data
- System lifecycle management
- Encryption

To take account of

- The security of systems and facilities
- Incident handling,
- Business continuity management
- Monitoring auditing and testing
- Compliance with international standards

NIS 2 Major Changes

Improved cybersecurity cooperation and capabilities

1

EU Member States

More stringent supervision measures and enforcement including fines.

2

Additional Industry Sectors

Scope of “essential entities” includes more sectors and services.

3

Security Measures

Risk analysis, incident handling, business continuity, supply chain, network, auditing.

4

Board Level Accountability

Regular training at the board level.

Art. 5 INational cybersecurity strategy

Art. 6 Coordinated vulnerability disclosure and a European vulnerability registry

Art. 7 National cybersecurity crisis management frameworks

Art. 14 The European cyber crises liaison organisation network (EU - CyCLONe)

Art. 18 Cybersecurity risk management measures

Art. 19 EU coordinated risk assessments of critical supply chains

Art. 20 Reporting obligations

Art. 21 Use of European cybersecurity certification schemes

3. Cyber Hygiene

The Foundation for Cyber Resilience

Cyber Hygiene – The Foundation

The essential elements that underpin cyber resilience

Cyber Hygiene	Area	Delivery		
Essentials		On Premises	IaaS	SaaS
Foundations	Identity and Access Management			
	Asset Management			
	Culture Responsibility and Training			

Cyber Hygiene – The Essentials

The essential elements that underpin cyber resilience

Cyber Hygiene	Area	Delivery		
Essentials	DR Planning and Incident Response	On Premises	IaaS	SaaS
	Data Protection & Data Backup			
	Privilege Management			
	Zero Trust Network Management			
	Vulnerability Management			
	Patch Management			
	Malware Protection			
Foundations	Identity and Access Management			
	Asset Management			
	Culture Responsibility and Training			

Incident Response Preparedness

IBM Cost of a Data Breach Report 2023

Top Cost Mitigators

- Dev Sec Ops Approach
- Employee Training
- **Incident Response Plan**

Top Cost Amplifiers

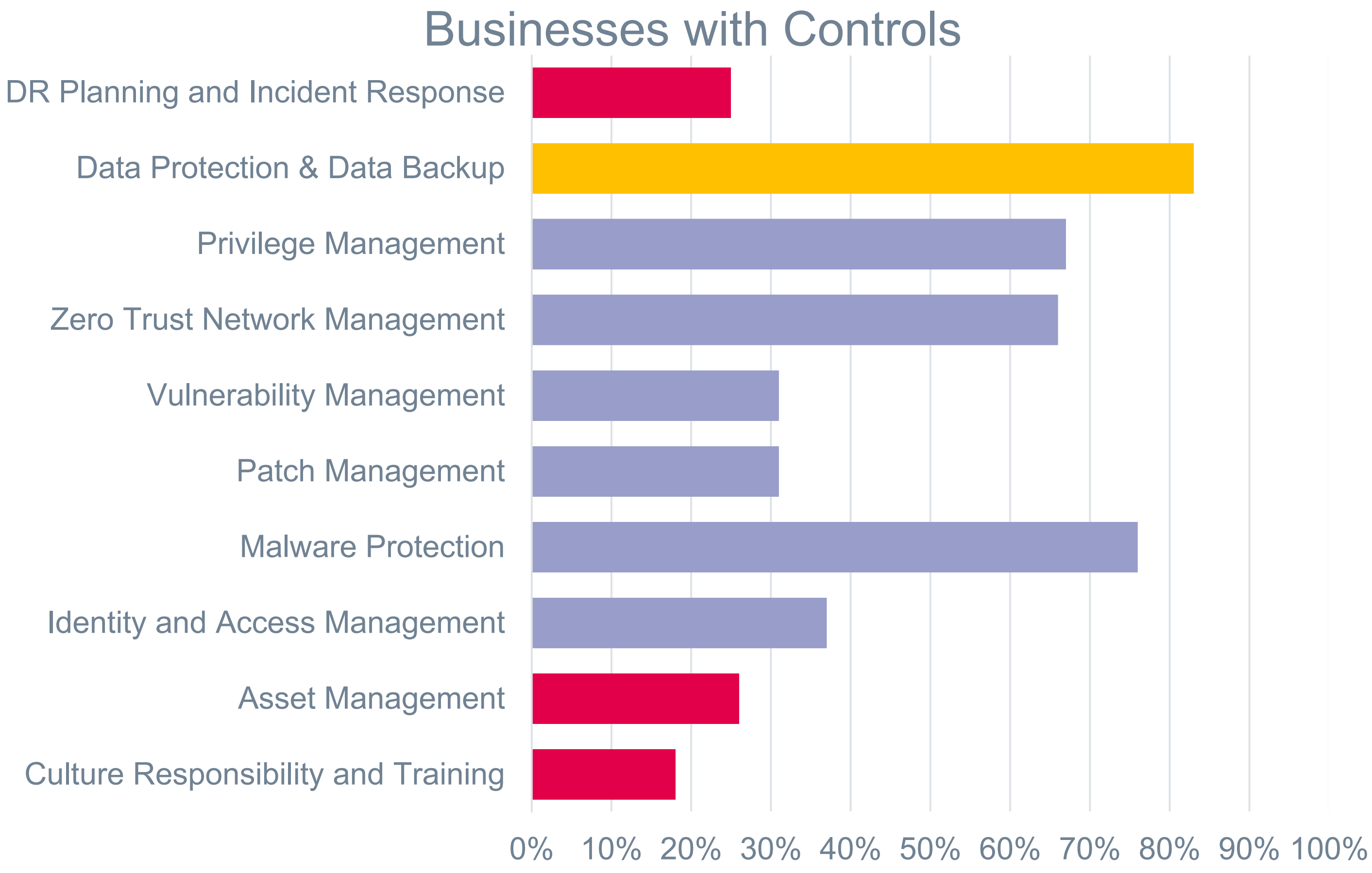
- **Non-compliance**
- Security Skills Shortage
- Security System Complexity

Cyber Hygiene in Practice

Results from UK NCSC Cyber Security Breaches Survey 2023

- 25% have a formal incident response plan
- 26% have a list of critical assets
- 83% organizations have cloud backups or other kinds of backups (Down from 2022)

Cyber Security Breaches Survey 2023 - GOV.UK (www.gov.uk)



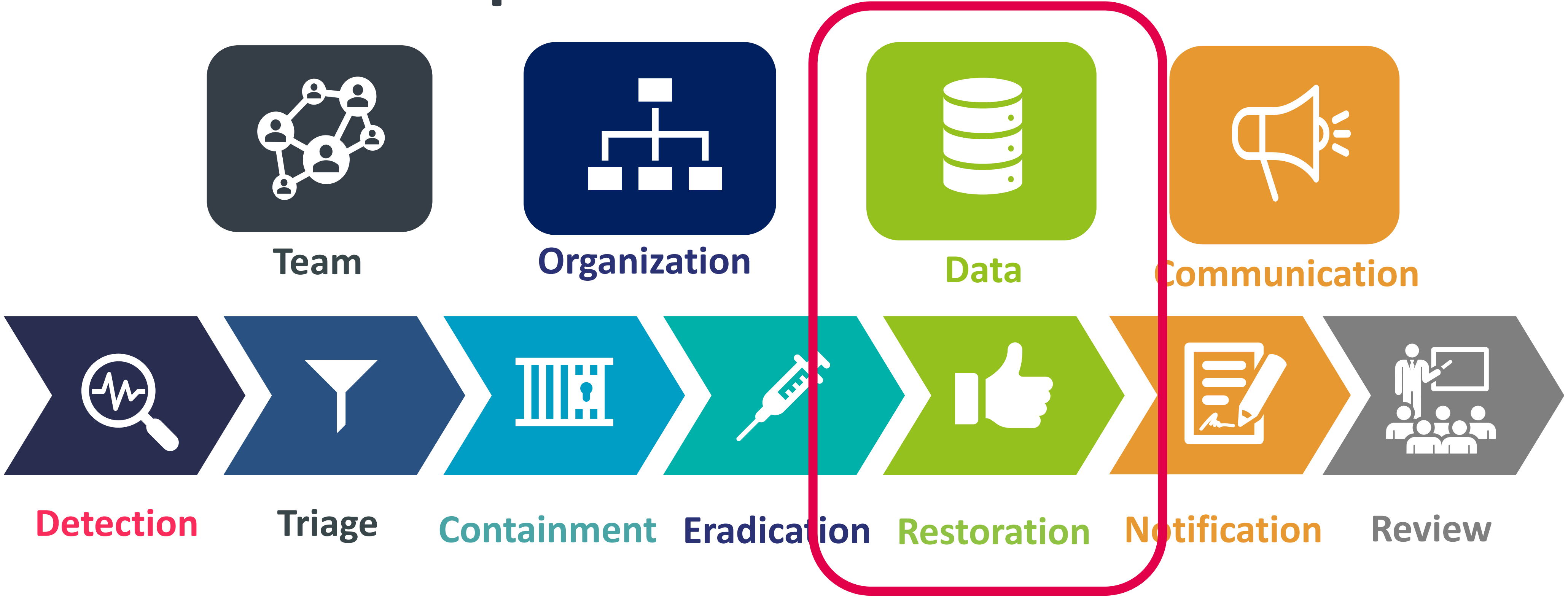
Incident Response

Fundamental component of cyber resilience

Be Prepared

A tested recovery plan is an essential part of Cyber Hygiene

Invest in Response as well as Prevention



Data Resilience

Data resilience is a critical part of cyber resilience

1

Services depend on business data

Without the business data the service has no value.

2

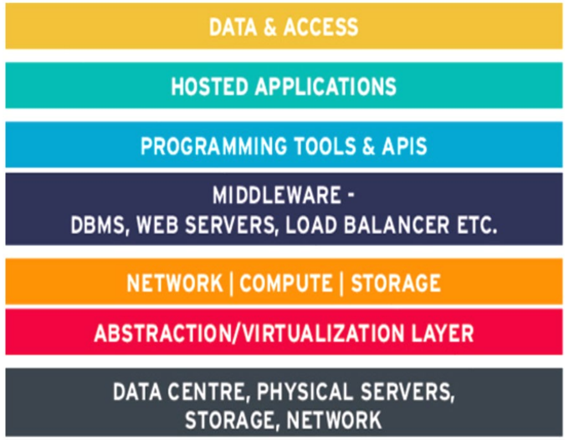
Services are defined by data - IaC

the structure of the services is data, and the software defined infrastructure depends on this.

3

No Data = No Service

Without data you cannot restore the services


DATA & ACCESS

HOSTED APPLICATIONS

PROGRAMMING TOOLS & APIS

MIDDLEWARE -
DBMS, WEB SERVERS, LOAD BALANCER ETC.

NETWORK | COMPUTE | STORAGE

ABSTRACTION/VIRTUALIZATION LAYER

DATA CENTRE, PHYSICAL SERVERS,
STORAGE, NETWORK

Myth - Cloud Services don’t need Backup

Responsibility for security is shared.

1

AWS S3 - 99.999999999% durability

But if you delete the data it is gone.

2

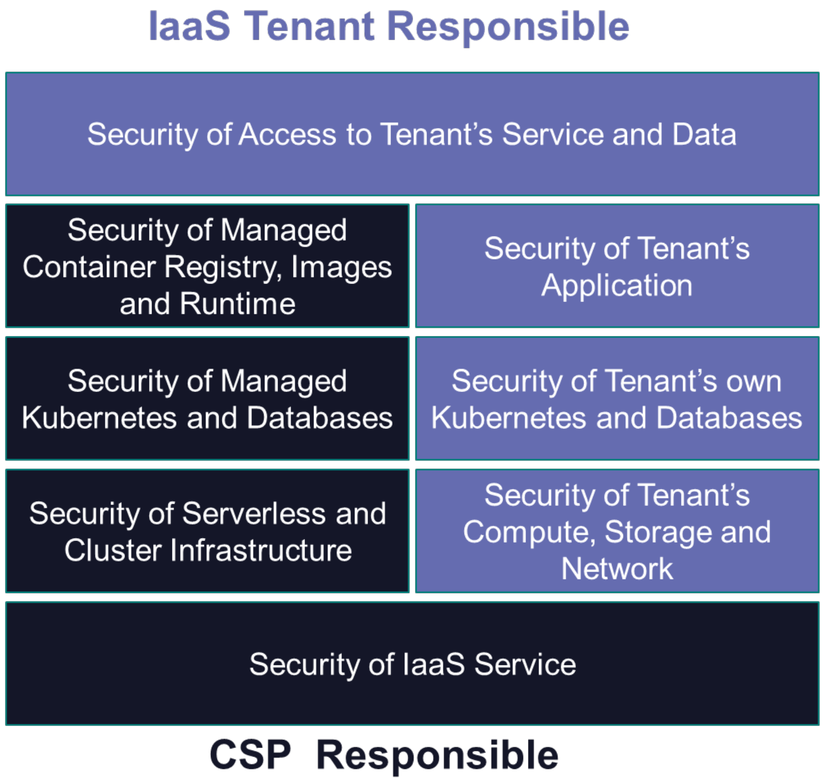
Office 365 – retains deleted data

For up to 30 days but if you delete from the recycle bin it is gone.

3

Cloud provides multiple availability zones

This only helps if you use them. If a data centre burns down, you could lose access.



IaaS Tenant Responsible

Security of Access to Tenant’s Service and Data

Security of Managed Container Registry, Images and Runtime

Security of Tenant’s Application

Security of Managed Kubernetes and Databases

Security of Tenant’s own Kubernetes and Databases

Security of Serverless and Cluster Infrastructure

Security of Tenant’s Compute, Storage and Network

Security of IaaS Service

CSP Responsible

Recovery depends upon Backup Data

Service restoration depends upon you having a clean backup of the data

Re-image

Restore

- Re-image affected systems
- Restore configurations
- Reset affected accounts
- Restore application data
- Change encryption keys

Re-test

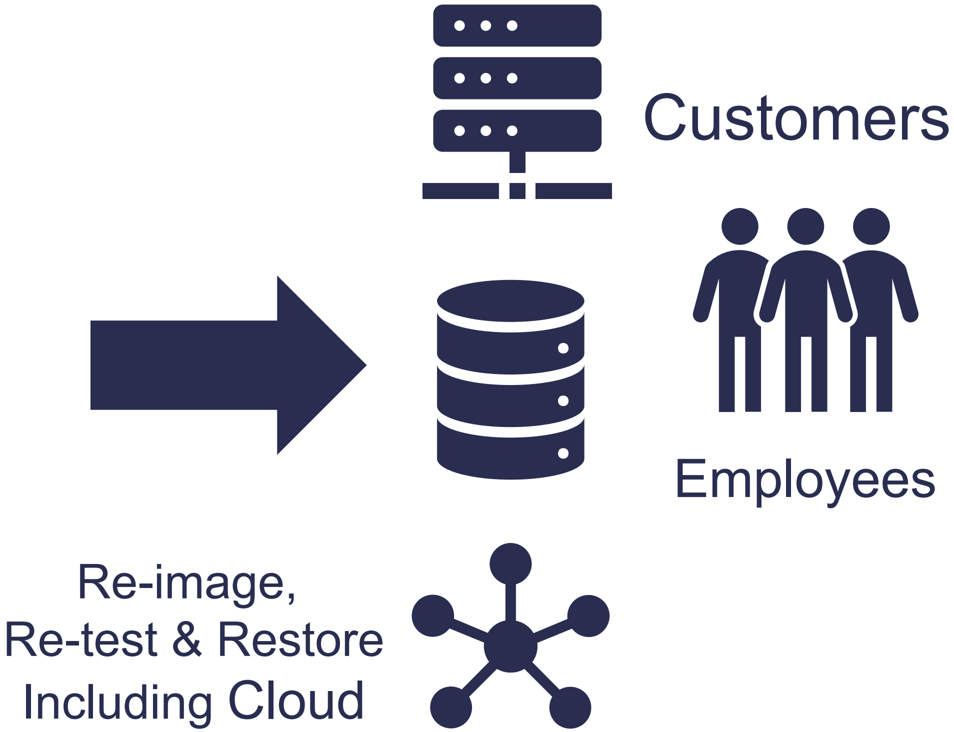
Retest affected systems

- Prove that the threats have been removed
- Test that the vulnerabilities have been removed
- Test that the systems are functional
- Check the integrity of the restored data

Restore Service

Restore the affected services

- Resume operation of affected applications, systems and data
- Monitor that functionality is correctly restored
- Monitor to ensure that threat is now cleared



Customers

Employees

Re-image,
Re-test & Restore
Including Cloud

Choosing a DR Solution

What are the capabilities to look for?

Basic Capabilities

For data resilience against ransomware and cyber threats

1

What is protected

Which data and applications on which service delivery methods are covered.

On Premises

IaaS

SaaS

2

Where the protected is data held

Which storage options are supported

Physical
(e.g. Tape)

Appliance
(Physical & Virtual)

In cloud

3

How recovery is achieved

Which recovery and restoration approaches are supported

DIY

DRaaS

Managed Service

Ransomware Protection

Proactive protection against ransomware attacks

Protect Data

Protect data against cyber attacks:

- Air Gap
- Object Lock
- Data integrity check

Protect Process

Protect backup process against attack:

- Strong authentication
- Hardened appliance
- Activity monitoring

Remove Malware

Detect and remove malware from protected data:

- Scan during backup
- Scan while stored
- Scan during download

Protect against the complex ransomware attack chain
Mitre ATT&CK MITRE ATT&CK®

Security

Essential security controls

Secure Transfer

Protect data in transit at least TLS 1.2.

Secure Storage

Protect data at rest certified encryption and customer control over keys.

Privilege Controls

Strong authentication for administrative access.

Delegation

Role Based access controls to enable secure delegation.

Auditability

Secure logging of administrative activity and the back-up processes.

Certification

Compliant with the laws and regulations required by the organization using it.

Deployments Protected

One stop coverage for hybrid IT

On Premises

Data and applications deployed on premises including:

- Physical and Virtual and SD infrastructure
- Databases
- Email / SharePoint
- Applications CRM, ERP, ..

IaaS

Data and applications deployed in:

- AWS
- Azure
- Google
- IBM Cloud
- Oracle
- …

SaaS

Range of services protected should include:

- Microsoft Office 365
- Google Workspace
- Salesforce.com
- Others

Disaster Recovery

How easily can you recover from the disruption

Range of DRaaS

Options available:

- Self-service - provides the tools needed.
- Assisted recovery – provides services and infrastructure.
- A fully managed service

Time to Recover

Meeting your Recovery Time Objectives:

- Guaranteed by SLA
- Techniques to minimize data transfers
- Synchronization
- Whole stack recovery

Compliance

DRaaS service should be independently certified / attested :

- ISO/IEC 27001
- PCI-DSS
- SSAE 18
- Other industry certifications

Data Resilience

For ransomware proof digital transformation

Summary

Secure and resilient digital transformation

Digitalization increases Cyber Risks

- Loss of Business Continuity.
- Data Breaches
- Compliance failure

Cyber Resilience

- An essential element of digital transformation.
- Needs good cyber hygiene.
- Increasing regulations.

Data Resilience

- IT Services are now Data Defined
- No Data = No Service.
- Be Prepared.

Data Resilience Solutions

- Recovery and Restoration.
- All data wherever it is.
- Test, test and test.

Leadership Compass: Cloud Backup for Ransomware Protection

THANKS!

Any questions?

KuppingerCole Analysts AG
Wilhelmstr. 20 - 22
65185 Wiesbaden | GERMANY

P: +49 | 211 - 23 70 77 - 0
F: +49 | 211 - 23 70 77 – 11

E: info@kuppingercole.com
www.kuppingercole.com