STADT BAD BERLEBURG

Mitteilungsvorlage	**Nummer 644-XI**	
Federführender Fachbereich: Zentrale Steuerung	**X**	**ÖT**
Az.: 10 - VS		**NÖT**

Anlagen: 3

Beratungsfolge	**Termin**	**Bemerkungen**
Haupt- und Finanzausschuss	08.02.2024	

Cyberangriff auf die Südwestfalen-IT: Aktueller Sachstand

Sachverhalt:

Die Aufgabenerledigungen in der Verwaltung werden durch den Cyberangriff auf die Südwestfalen-IT (SIT) seit dem 29. Oktober 2023 massiv beeinflusst. Eine erste Einschätzung, auch zum voraussichtlichen Ablauf des Hackerangriffes, erfolgte bereits in der Stadtverordnetenversammlung am 30. Oktober 2023. Im Haupt- und Finanzausschuss am 14.12.2023 erfolgte ein erneuter Bericht zum aktuellen Stand. Der bei der Stadt Bad Berleburg dazu eingerichtete Stab für außergewöhnliche Ereignisse (SAE) trifft sich nach anfänglich höherer Frequenz nun mindestens 1x wöchentlich, um die Entwicklungen und Maßnahmen aufeinander abzustimmen.

Projektmanagement in Bad Berleburg:

Die Verwaltung der Stadt Bad Berleburg konnte bereits kurz nach dem Cyberangriff eine weitgehend stabile Kommunikationsstruktur und technische Notfallsysteme, gesteuert über den SAE, aufbauen. Dank unserer IT-Abteilung, den Möglichkeiten aus dem Smart-Cities-Projekt sowie dem besonderen Engagement der Kolleginnen und Kollegen war und ist die Stadt Bad Berleburg hier auf einem guten Weg bzw. es konnten im Sinne der Bürgerinnen und Bürger bislang gute Lösungen gefunden werden. Auch die interkommunale Zusammenarbeit, z.B. mit der Stadt Hatzfeld, hat hier geholfen, zumal mit der Stadt Hatzfeld bereits im Sommer 2023 ein solches Szenario mit den möglichen Optionen durchgesprochen wurde. Es erfolgten zudem enge Abstimmungen mit den Kommunen im Kreis Siegen-Wittgenstein und der SIT.

Der Bürgermeister

Bernd Fuhrmann

_____

Zahlreiche Anwendungen sind aber noch im Basis-Betrieb, sodass dort noch nicht alle üblichen Nutzungen möglich und nicht alle Daten vorhanden sind.

Das Beispiel Finanzsoftware macht Hoffnung:
Nachdem nach dem Angriff Ende Oktober sämtliche Fachsoftware der Verwaltung nicht mehr zur Verfügung stand, wurde die Finanzsoftware INFOMA mit wesentlichen Komponenten zu Beginn der 51. KW in 2023 wieder zur Verfügung gestellt. Unmittelbar nach Wiederherstellung der Software konnte festgestellt werden, dass alle wesentlichen Inhalte und Buchungsstände aus der Zeit vor dem Cyberangriff gesichert werden konnten und wieder zur Verfügung stehen.

Der Infoma-Normalbetrieb mit allen Komponenten soll bis Ostern wieder funktionieren. Dies gilt auch für das Ratsinformationssystem SD-Net, sodass zur nächsten Plenarwoche vermutlich wieder das Ratsinformationssystem genutzt werden kann.

Die übrigen Fachverfahren werden je nach Dringlichkeit entsprechend einer Prioriätenliste neu aufgesetzt. Hier gilt es dann jeweils mit entsprechendem Aufwand die seit Ende Oktober erfolgten Verwaltungsvorgänge einzuarbeiten bzw. diese entsprechend zu verzahnen.

Der aktuelle Stand der Wiederanlaufplanung ergibt sich aus der Präsentation in der vergangenen Sitzung der SIT-Gesellschafterversammlung am 25.01.2024, welche als **Anlage 1** beigefügt ist. Grundsätzlich soll bei den Anwendungen auf einen gesicherten Datenbestand zwischen dem 14. und dem 29. Oktober 2023 zurückgegriffen werden.

Der Wiederaufbau der Basisinfrastruktur und der Fachverfahren wird noch auf absehbare Zeit viele Ressourcen binden.

Forensischer Bericht zur Cyberattacke:

In der SIT-Gesellschafterversammlung am 25.01.2024 wurde der abschließende Forensik-Bericht des von der SIT beauftragten Unternehmens r-Tec vorgelegt. Die dazugehörige Präsentation mit den wesentlichen Aussagen ist als **Anlage 2** beigefügt. Der Gesamtbericht ist über die Notfall-Homepage der SIT abrufbar:
https://notfallseite.sit.nrw/fileadmin/user_upload/SIT_Incident_Response_v1.1.pdf

Dabei wurden entsprechende Sicherheitslücken deutlich, welche den Angreifern von Akira, einer weltweit bekannten und professionellen Cybergang, das Eindringen erleichtert haben (u.a. keine Multifaktor-Authentifizierung bei VPN-Nutzung, einfache Entschlüsselung der SIT-Gruppenrichtlinie mit der Möglichkeit des Zugangs zu Admin-Rechten etc.). Ein Datenabfluss ist nach den bisherigen Erkenntnissen nicht erfolgt.

Lösegeld wurde im Übrigen nicht gezahlt, da sich der Staat – und damit auch ein kommunaler Zweckverband – grundsätzlich nicht erpressen lassen kann.

Die SIT hat zudem angekündigt, ihre Kommunikation deutlich zu verbessern, da es dazu deutliche Kritik von den betroffenen Kommunen gibt.

Unabhängig davon ist festzuhalten, dass neben Kommunen auch viele Unternehmen täglich erfolgreich von Cyberangriffen betroffen sind, wobei die Dunkelziffer durch vermutliche Lösegeldzahlungen hoch sein dürfte. Aufgrund des Fachkräftemangels, den im IT-Sektor auch deutlich die SIT spürt, und der weiteren landesweiten Digitalisierungsstrategie ist davon auszugehen, dass es weitere Kooperationen bzw. Fusionen von IT-Dienstleistern in NRW geben wird.

Die Aufarbeitung der Situation bei der SIT und die weitere Strategie soll im Wesentlichen durch den neuen Geschäftsführer Mirco Pinske angesteuert werden, der am 01. Februar 2024 seinen Dienst angetreten hat. Herr Pinske verfügt als Diplom-Kaufmann über langjährige Erfahrungen als Führungskraft und gilt als Experte für Prozessoptimierung. Die Entscheidung zur Bestellung von Herrn Pinske in der Nachfolge des bisherigen Geschäftsführers Thomas Coenen, der die SIT auf eigenen Wunsch zum 30.09.2023 verlassen hatte, erfolgte bereits am 24. Oktober 2023, also unmittelbar vor dem Cyberangriff.

Finanzielle Auswirkungen:

Die konkreten finanziellen Auswirkungen bei der Stadt Bad Berleburg sind derzeit noch nicht zu beziffern. Ziel ist es, die bei der Stadt Bad Berleburg angefallenen Kosten näherungsweise zu erfassen. Hinzu kommen die auf den Zweckverband SIT zusätzlichen Kosten, bei dem alle Kommunen in Südwestfalen Mitglied sind und insofern auch die Stadt Bad Berleburg einen Anteil trägt. Generell ist davon auszugehen, dass in die IT-Sicherheit in Zukunft deutlich mehr zu investieren ist.

Externe Schadensersatzansprüche wurden gegenüber der Stadt Bad Berleburg bislang nicht geltend gemacht. Die SIT hatet nach Abwägung von Aufwand und Nutzen keine separate Cyberversicherung abgeschlossen.

Die SIT lässt derzeit juristisch prüfen, ob und wie die durch den Cyberangriff ausgelösten Schäden ggf. geltend gemacht werden können. Das Ergebnis wird den Kommunen mitgeteilt, um dort dann entsprechende Entscheidungen hinsichtlich Schadensersatz treffen zu können.

Um die Liquidität bei der SIT zu gewährleisten, haben der Verbandsvorsteher und die Geschäftsführung mit Schreiben vom 18.01.2024 **(Anlage 3)** darum gebeten, die Entgeltzahlungen auch in 2024 zu leisten, obwohl entsprechende Leistungen nicht oder nicht umfänglich erbracht werden konnten. Es wurde im Bewusstsein einer rechtlichen Grauzone durch den Verbandsvorsteher, Landrat Theo Melcher, und die Vorsitzende der Verbandsversammlung, Landrätin Eva Irrgang, in der Sitzung des SIT-Verwaltungsrates für die aufgezeigte pragmatische Vorgehensweise in dieser Krisensituation geworben und zugesichert, dass später durch entsprechende Gremienbeschlüsse die Rechnungen korrigiert bzw. etwaige Überzahlungen verrechnet werden. Derzeit müsse die Kraft in das Wiederanlaufen der Systeme gesteckt werden. Da den Kommunen zudem schriftlich zugesichert wurde, dass durch die Zahlungen keine Nachteile entstehen und die Kommunen selbst Mitglied im Zweckverband der SIT sind, beabsichtigt auch die Stadt Bad Berleburg dieser Vorgehensweise zu folgen.

Sachstandsbericht zur Cyberattacke – Wiederanlaufplanung

Verwaltungsrat/Verbandsversammlung am 25.01.2024

Autor: **Jörg Kowalke**

Version: freigegeben
1.0

Agenda

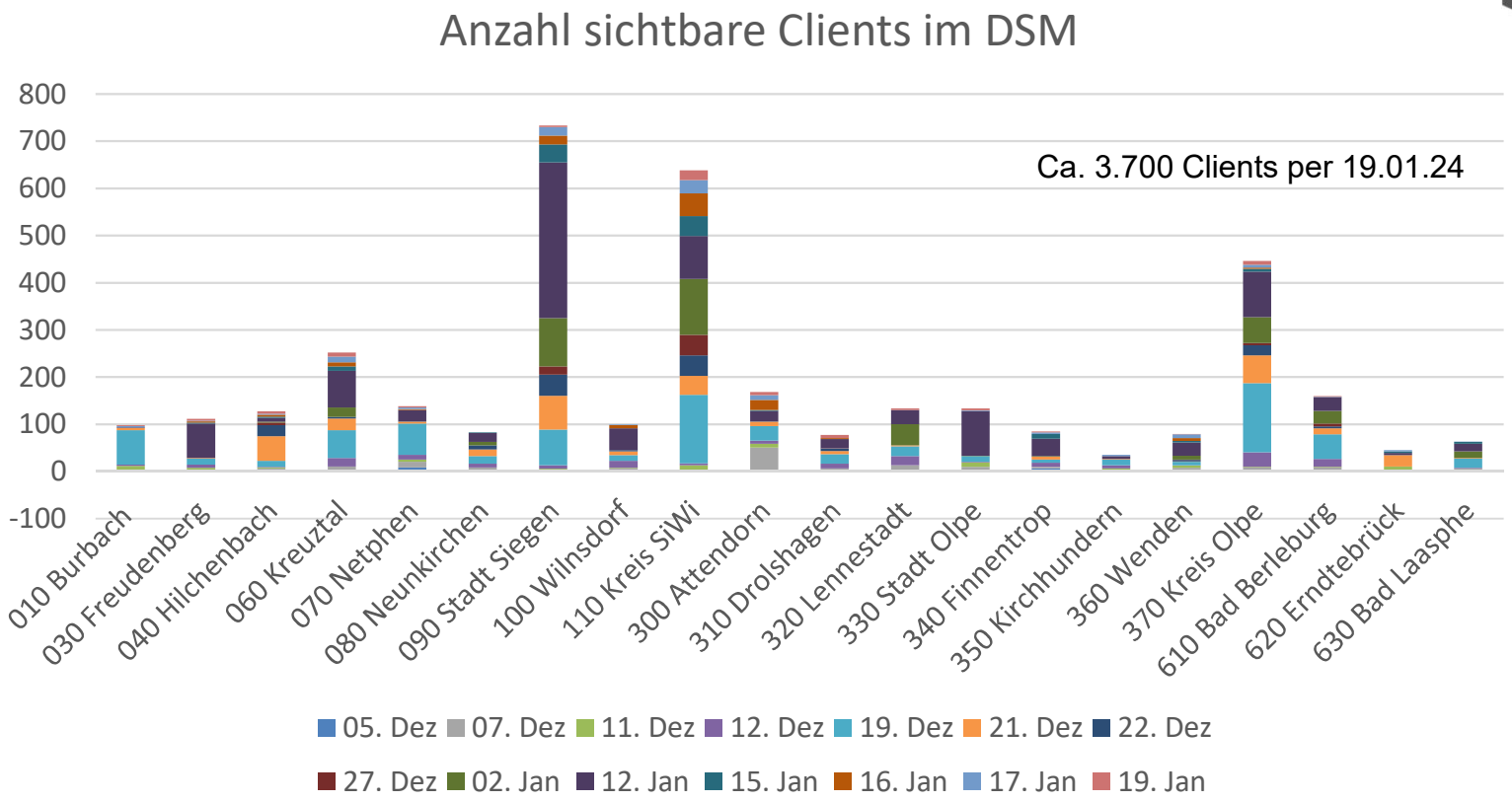
- Status Infrastruktur
- Planung Fachverfahren
- Ausblick

Status - Infrastruktur

- Mobiler Zugriff Kalender und Mail – im Rollout im Nordverband

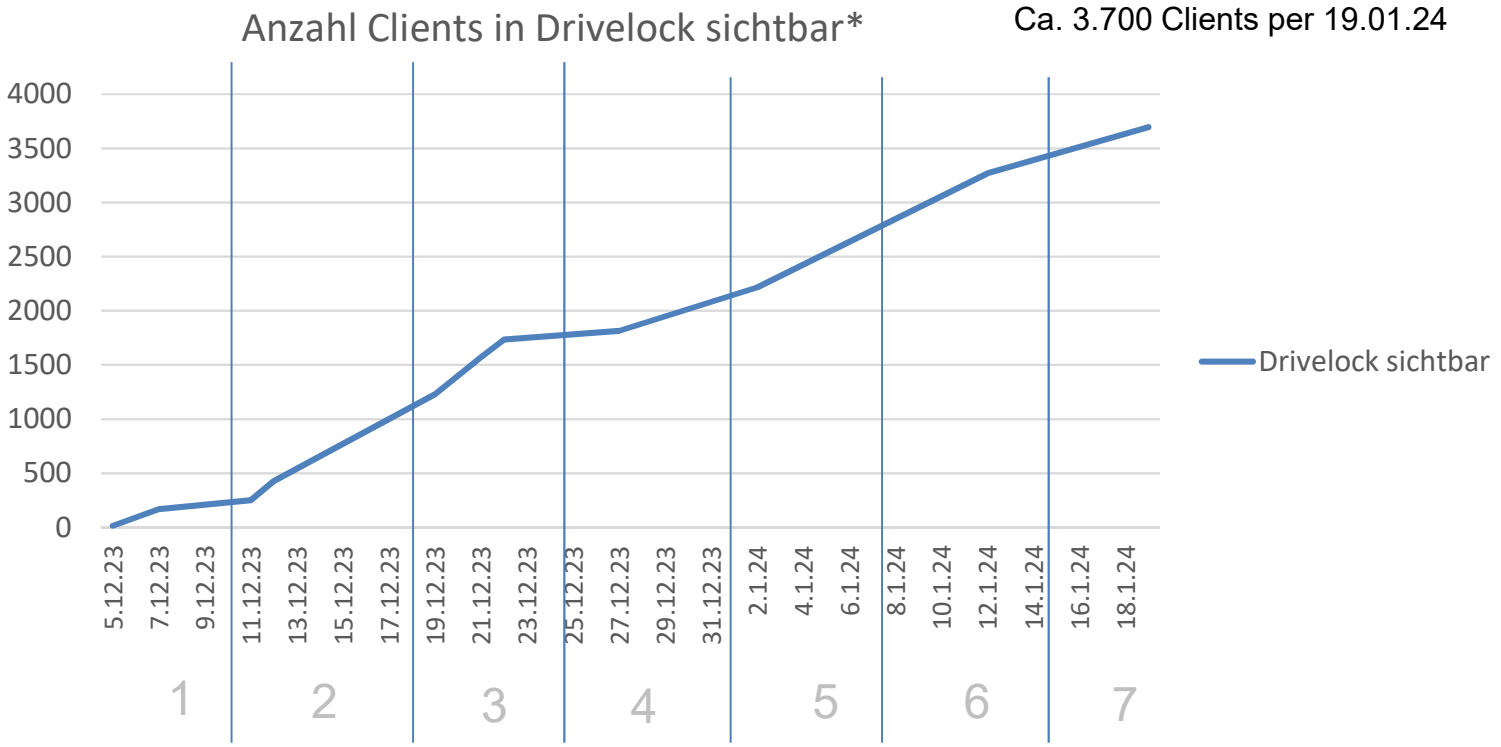
- Status NOT.LAN
  - Aufbau Mail
    - Aufbau leere Standard-Postfächer erfolgt – Bereitstellung Altdaten: im Rollout
  - Aufbau Fileserver
    - Aufbau leerer Fileserver je Kommune erfolgt – Bereitstellung Altdaten: im Rollout
  - Anbindung separat angebundene Außenstellen
    - Anbindung in Arbeit – z.T. wird Hardware ausgetauscht
  - Aufbau Druckserver
    - Druckserver pro Verwaltung ist in Arbeit
  - Neuaufbau Client
    - Aufbau läuft – derzeitiger Stand ca. 3.700 Clients

Aufbau not.lan - Entwicklung Clients



* Typische Voraussetzung: Grundinstallation in DSM ist erfolgreich

Stand Clients



* Typische Voraussetzung: Grundinstallation in DSM ist erfolgreich

Planung - Fachverfahren
Zeitplanung Anlauf Normalbetrieb

Fachverfahren	Nutzer	Betreiber	Basis-betrieb	Phase 1	Normal-betrieb
KDN.Sozial	Nord+Externe	SIT	Live	KW 5	KW 12
Inforegister	Nord+Externe	SIT	Live	./.	KW 9
VOIS|MESO	Nord+Externe	SIT	Live	KW 5	KW 9
ADVIS	Nord+Süd+Externe	SIT	Live	KW 7	KW 13
OK.Verkehr	Nord+Süd	regio iT	Live	KW 9	KW 16
OK.EWO	Süd	SIT	Live	KW 5	KW 9
Autista/ePR	Nord+Süd+Externe	SIT	Live	Live	KW 8
infoma	Nord+Süd+Externe	SIT	Live	KW 5	KW 12
MACH	Nord+Extern	SIT	Live	KW 5	KW 8
WG Plus	Nord+Externe	SIT	Live	./.	KW 10
CZ Wohngeld	Süd	regio iT	KW 5	./.	KW 12

Phase 1 => erste Erweiterung Funktionsumfang / Schnittstellen

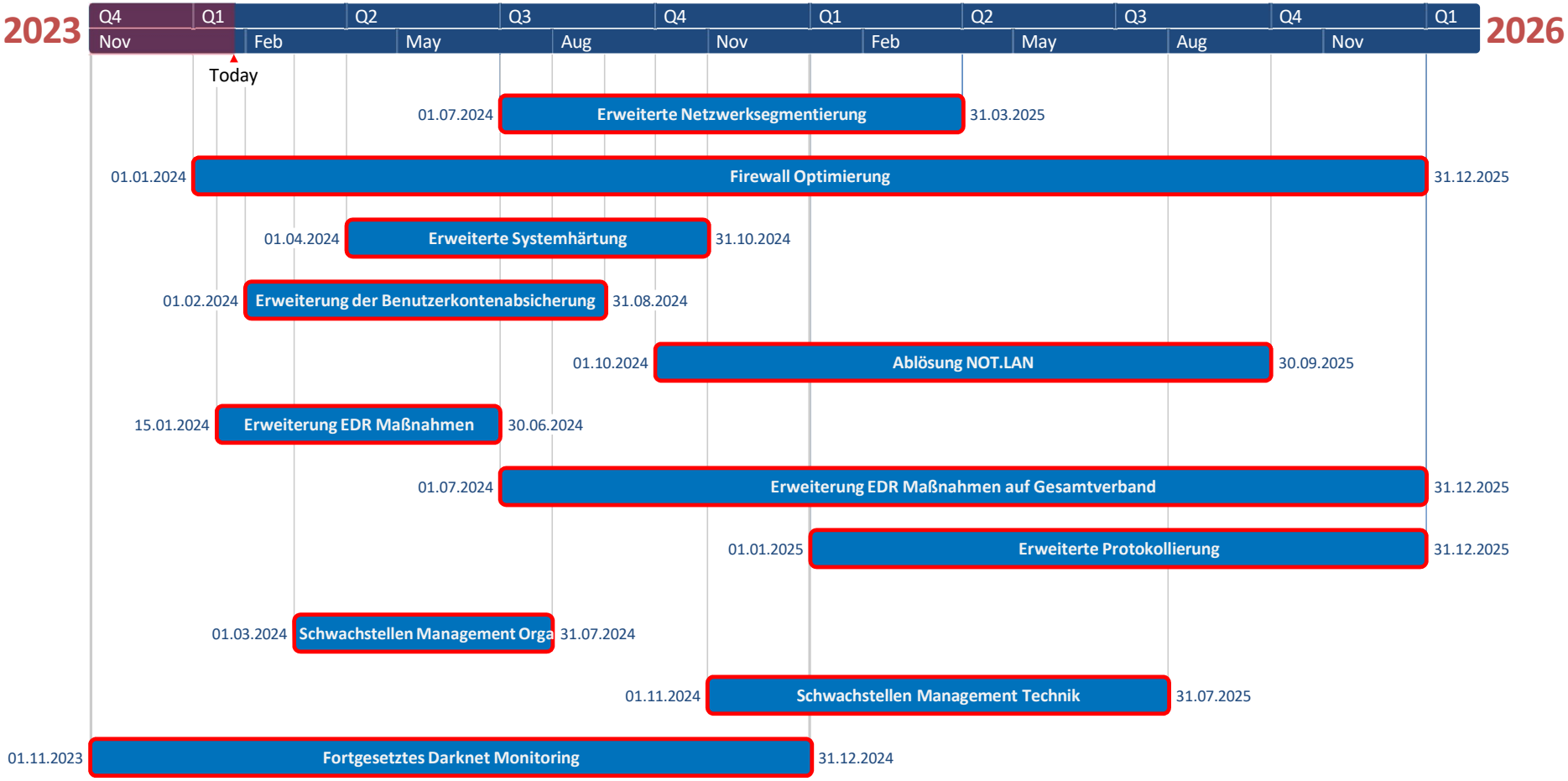
Ausblick - Fachverfahren Priorität 2

Verfahren	Info	Nutzer	Betreiber	Basis-betrieb	Normal-betrieb
SD.NET	Abstimmung mit KDVZ Frechen	Süd	Prüfung	KW 10	tbd
SC-OWI	Wiederanlauf	Nord	SIT	KW 05	KW 14
WinOWIG	Neuaufbau	Nord & Süd	SIT	KW 07	KW 14
VoteManager	Auslagerung zur KDVZ Frechen	Nord & Süd		KW 04	KW 07
ProSozBau (ProBauG)	Neuaufbau	Süd	SIT	KW 04	KW 13
ALKIS	Neuaufbau	Süd	SIT	KW 13	KW 22
beBPo	Wiederanlauf	Nord & Süd	SIT	KW 05	KW 07
citkoPortal / Form-Solutions	Nur Serveranlauf, Betrieb durch nextgov iT	Nord & Süd	SIT / nextgov iT	KW 05	KW 10
Doxis	Wiederanlauf	Nord	SIT	KW 09	tbd
Enaio	Neuaufbau	Süd	SIT	KW 09	KW 18
Loga	Extern krz, bereits lauffähig	Nord & Süd	OWL-IT	2023	2023
Migewa	Auslaufbetrieb wg. Migration VOIS|GESO	Süd	Prüfung		tbd
WinBIAP	Wiederanlauf	Nord & Süd	SIT	KW 14	KW 18
VOIS|GESO	Wiederanlauf	Nord	SIT	KW 05	KW 18
Vollstreckung Infoma	Neuaufbau	Nord & Süd	SIT	KW 13	tbd

Ausblick - Infrastruktur Priorität 2

Verfahren	Info	Nutzer	Betreiber	Basis-betrieb	Normal-betrieb
Transfer CI	Wiederanlauf	Nord & Süd	SIT	live	KW 07
UC4	Wiederanlauf	Nord & Süd	SIT	KW 04	KW 07
Client VPN	Neuaufbau	Nord & Süd	SIT	./.	KW 13
Active Sync Nord	Wiederanlauf	Nord	SIT	./.	Live
V-PKI	Wiederanlauf	Nord & Süd & Ex	SIT	./.	KW 05
MFA alle Win-Domänen	Neuaufbau	Nord & Süd	SIT	./.	KW 06
Wiki Verband	Wiederanlauf	Nord & Süd	SIT	./.	KW 04
Ticket-Front-End SITE	Wiederanlauf	Nord & Süd	SIT	./.	live
MDM	Wiederanlauf	Nord & Süd	SIT		KW 13
Druckserver not.lan	Neuaufbau	Süd	SIT	KW 05	KW 09
Datenrücksicherung Fileserver not.lan	Neuaufbau	Süd	SIT	KW 04	KW 09
Datenrücksicherung Exchange-Postfächer	Neuaufbau	Süd	SIT	KW 05	KW 13

Mittelfristige Sicherheitsmaßnahmen



Fragen?

Ihr Ansprechpartner/in: Jörg Kowalke

S-IT – Verwaltungsrat / Verbandsversammlung, 25.01.2024

ABSCHLUSSBERICHT SECURITY INCIDENT

Reframe your readiness.

Marek Stiefenhofer
Geschäftsführender Gesellschafter

AGENDA

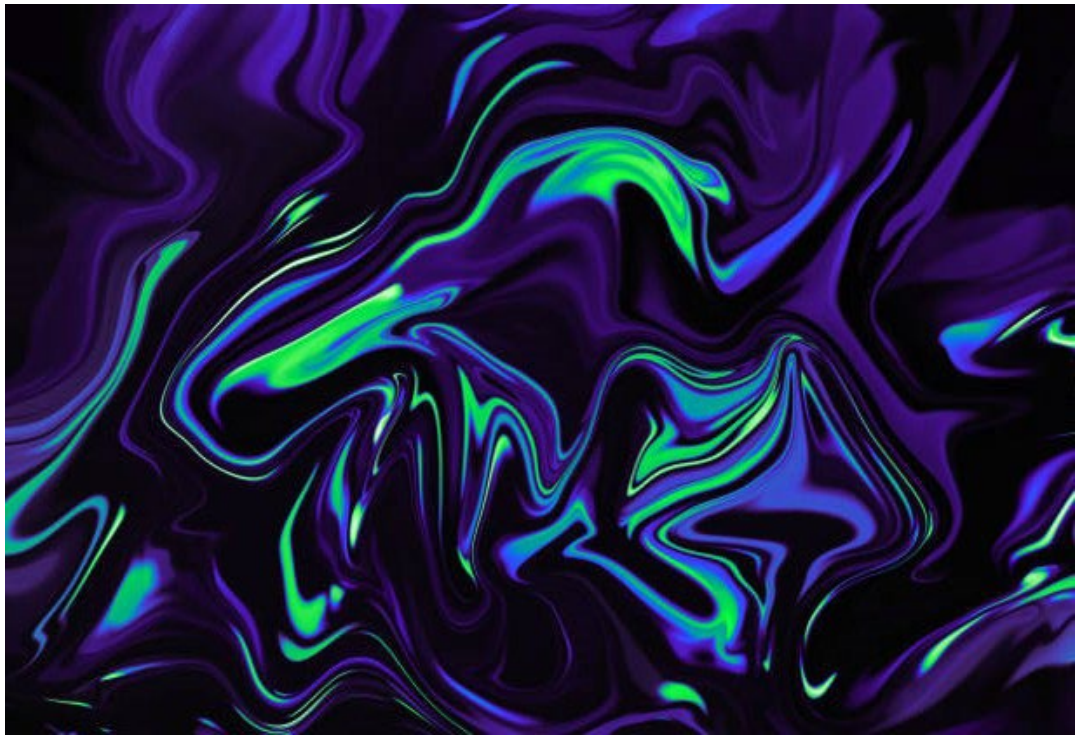
1 **Scope**

2 **Incident Management Timeline**

3 **Ablauf des Angriffs**
Initialer Eintrittsvektor
Ausbreitung und Rechteerweiterung
Ausführung der Ransomware

4 **Risikobewertung → Wiederherstellung**
Backup-Situation
Persistenz im Netzwerk
Bewertung Datenabfluss

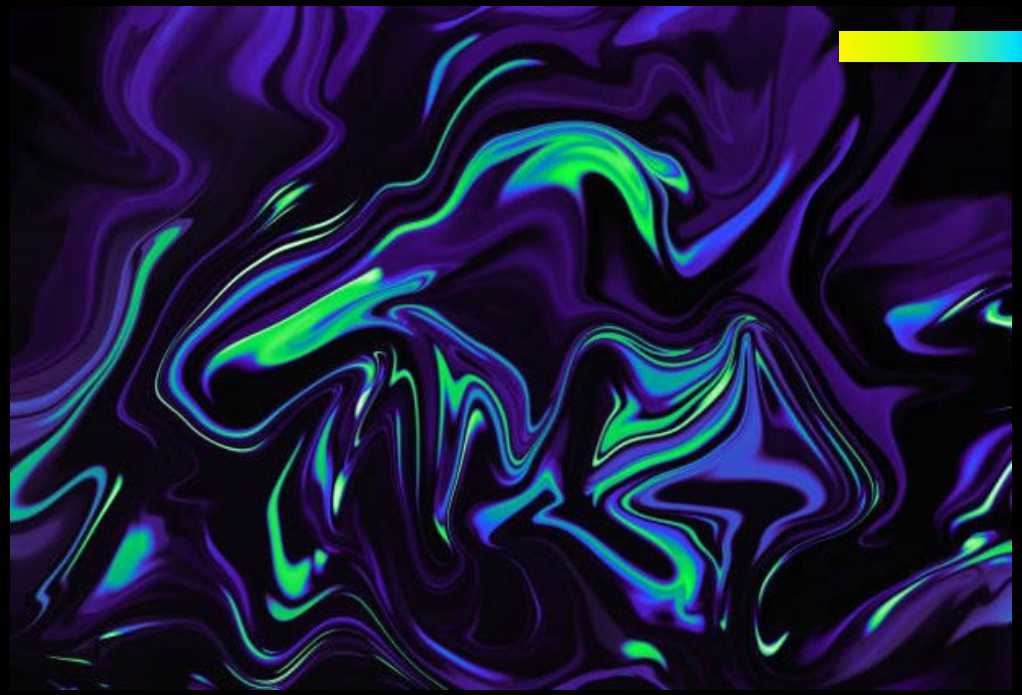
5 **Verbesserungsmaßnahmen**
Implementierte und geplante Maßnahmen



01

SCOPE

Reframe your readiness.



HINWEIS

Diese Präsentation ist nur eine Zusammenfassung des detaillierten Forensik-Abschlussberichtes, der S-IT am 22.01.2024 vorgelegt wurde.

UNTERSUCHUNGSGEGENSTAND

Untersuchungsobjekt	Zusätzliche Informationen
intra.lan Domäne	▸ 770 Server ▸ 4.176 Clients
sit.dl Domäne	▸ 41 Server ▸ 271 Clients
citkomm.local Domäne	▸ 19 Server
DMZ	▸ 320 Server
kdvz-bb.local Domäne	▸ 30 Server
bb.citkomm.de Domäne	▸ 105 Server
Diverse Netz-BB Server	▸ 374 Server
Diverse Infrastruktur	Cisco ASA Firewall Logs, Cisco ISE Authentifizierungs Logs, MikroTik Router Logs, Proxy Logs, Symantec Endpoint Protection Logs, F-Secure Endpoint Protection Logs

02

INCIDENT MANAGEMENT TIMELINE

Reframe your readiness.

INCIDENT MANAGEMENT TIMELINE (1 / 2)

18.10.2023

- Erste identifizierte Angreifer-VPN-Sitzungen

29.10.2023

- Verschlüsselung von Dateien durch Ransomware

30.10.2023, 02:00 – 06:30

- Sämtliche Server heruntergefahren
- Verbindungen zu Kunden gekappt
- Internetverbindung gekappt

30.10.2023, 08:00

- Entscheidung getroffen, r-tec zu beauftragen

INCIDENT MANAGEMENT TIMELINE (2 / 2)

30.10.2023, 11:00 – 12:00

- Gemeinsame Konferenz zur Abstimmung des weiteren Vorgehens

30.10.2023, 14:00 Uhr

- Eintreffen der ersten Forensiker und Incident Manager bei SIT in Siegen

30.10.2023 – 31.12.2023

- Forensik

30.10.2023 - fortlaufend

- Unterstützung Wiederaufbau
- Sicherheitsempfehlungen

03

ABLAUF DES ANGRIFFS

- Initialer Eintrittsvektor
- Laterales Bewegen, Erhöhung der Privilegien
- Ausführung der Ransomware

Reframe your readiness.

INITIALER EINTRITTSVEKTOR

ERSTER ZUGANG ERFOLGTE PER CISCO VPN

- Nachweislich ab 18.10.2023 war der Angreifer im Besitz von VPN Zugangsdaten
- Die VPN Sessions sind die ersten nachweisbaren Angreiferaktivitäten
- Angreiferzugriffe können nur per Geo-Location der IP-Adresse und VirtualBox-MAC-Adressen von legitimen VPN Sessions unterschieden werden

UNGEKLÄRTE BESCHAFFUNG DER ZUGANGSDATEN

Verschiedene mögliche Szenarien:

- Phishing: Keine Anzeichen für Phishing in den betr. Mailboxen gefunden
- Darkweb-Handel: Keine S-IT Artefakte in der Darkweb-Suche entdeckt
- Brute-Force: Wahrscheinlichstes Szenario

BRUTE-FORCE-SZENARIO

- Es gab Anzeichen für vermehrte Anmeldeversuche vor dem Angriff
- Cisco ASA Schwachstelle CVE-2023-20269 erleichtert Brute-Forcing
- S-IT war von der Schwachstelle betroffen
- Akira hat sich auf diese Schwachstelle in Kombination mit fehlender MFA „spezialisiert“

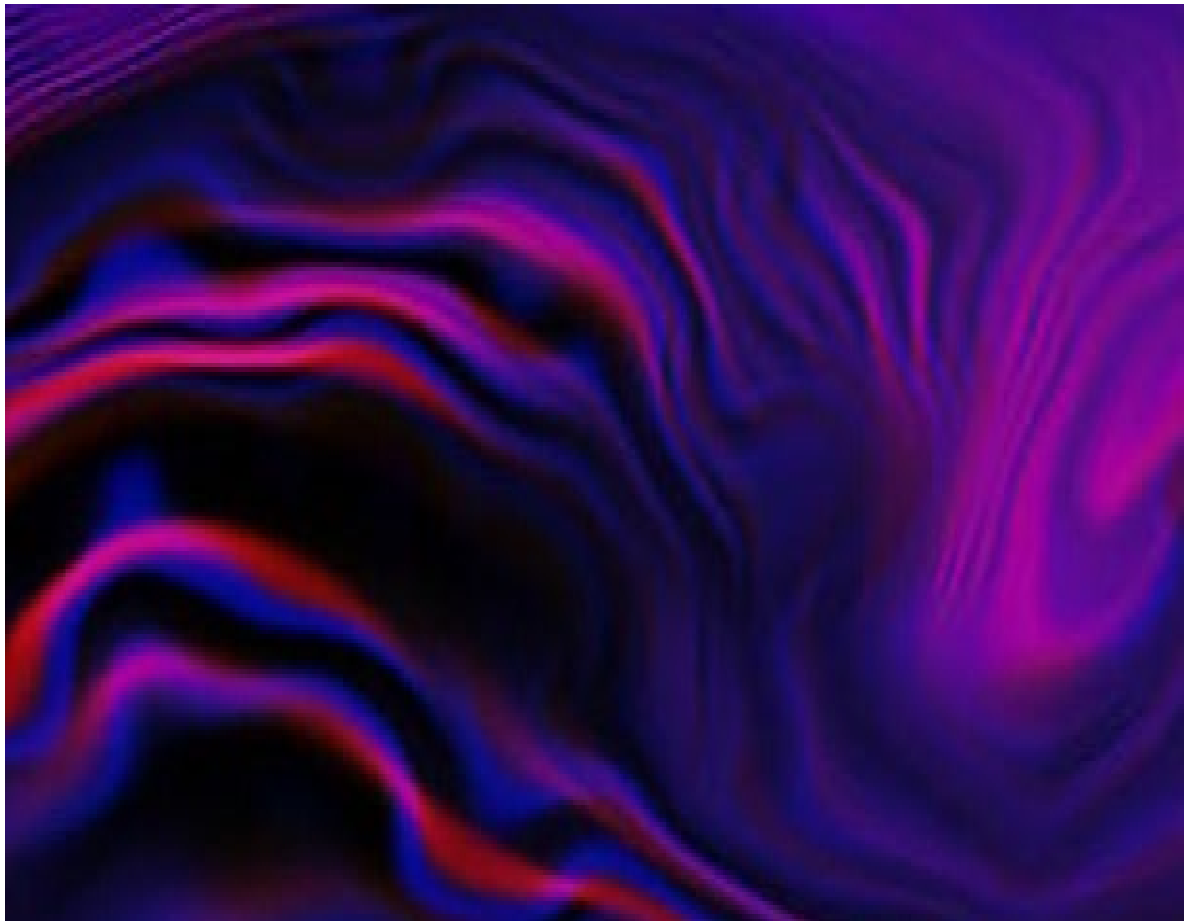
AUSBREITUNG UND RECHTEERWEITERUNG: FORENSISCHER ANSATZ

S-IT hat alle existenten Logs umgehend für die Forensik bereitgestellt.

Event-Logs reichten jedoch nicht aus, um das Angreifer-verhalten nach dem initialen Eintritt vollständig zu rekonstruieren, insbesondere:

- **Windows Event-ID 4624**
- **Firewall Logs innerhalb des Netzwerkes**

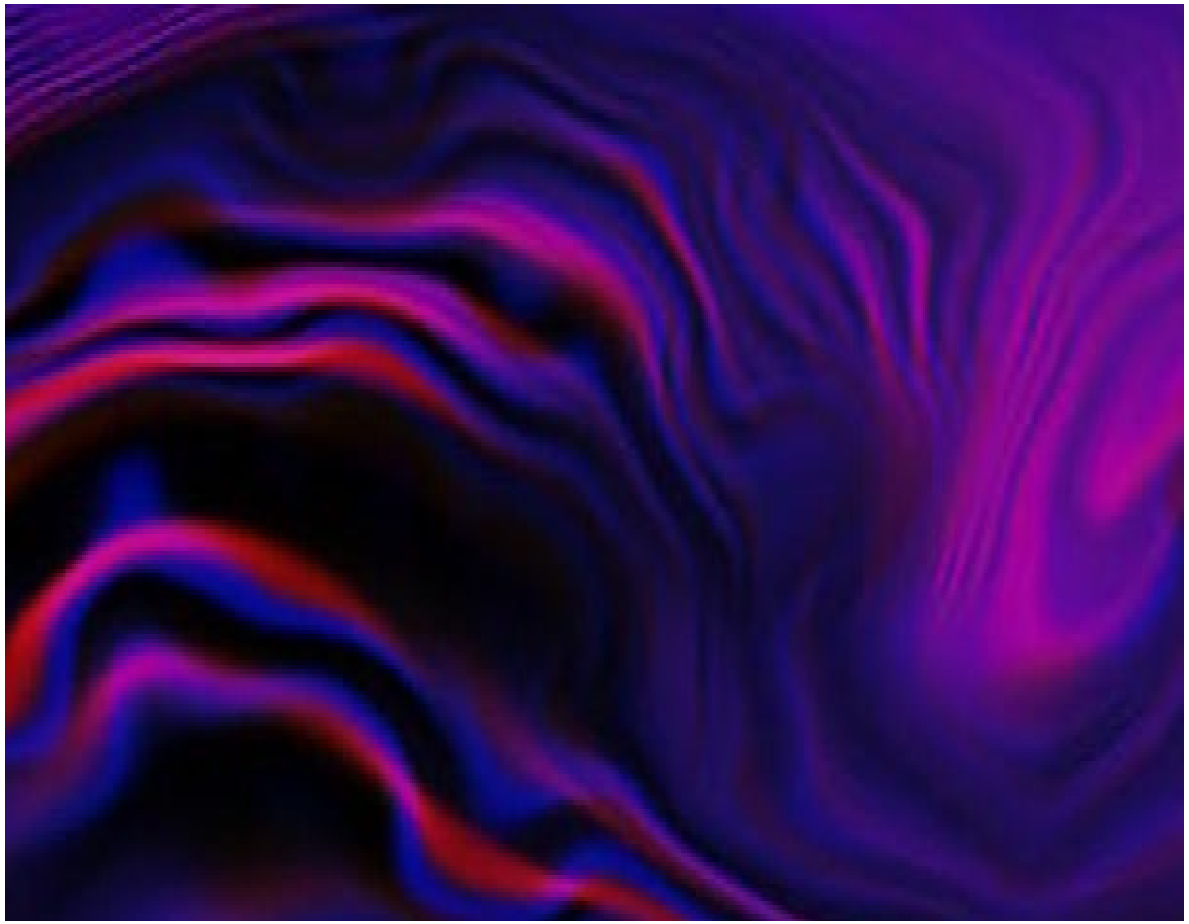
- **18.10.2023:**
  fehlgeschlagene Anmeldeversuche auf 190 verschiedene Server
- **18.10. – 29.10.2023:**
  keine Hinweise auf typische Methoden zur Erhöhung der lokalen Berechtigungen oder laterales Bewegen im Netzwerk

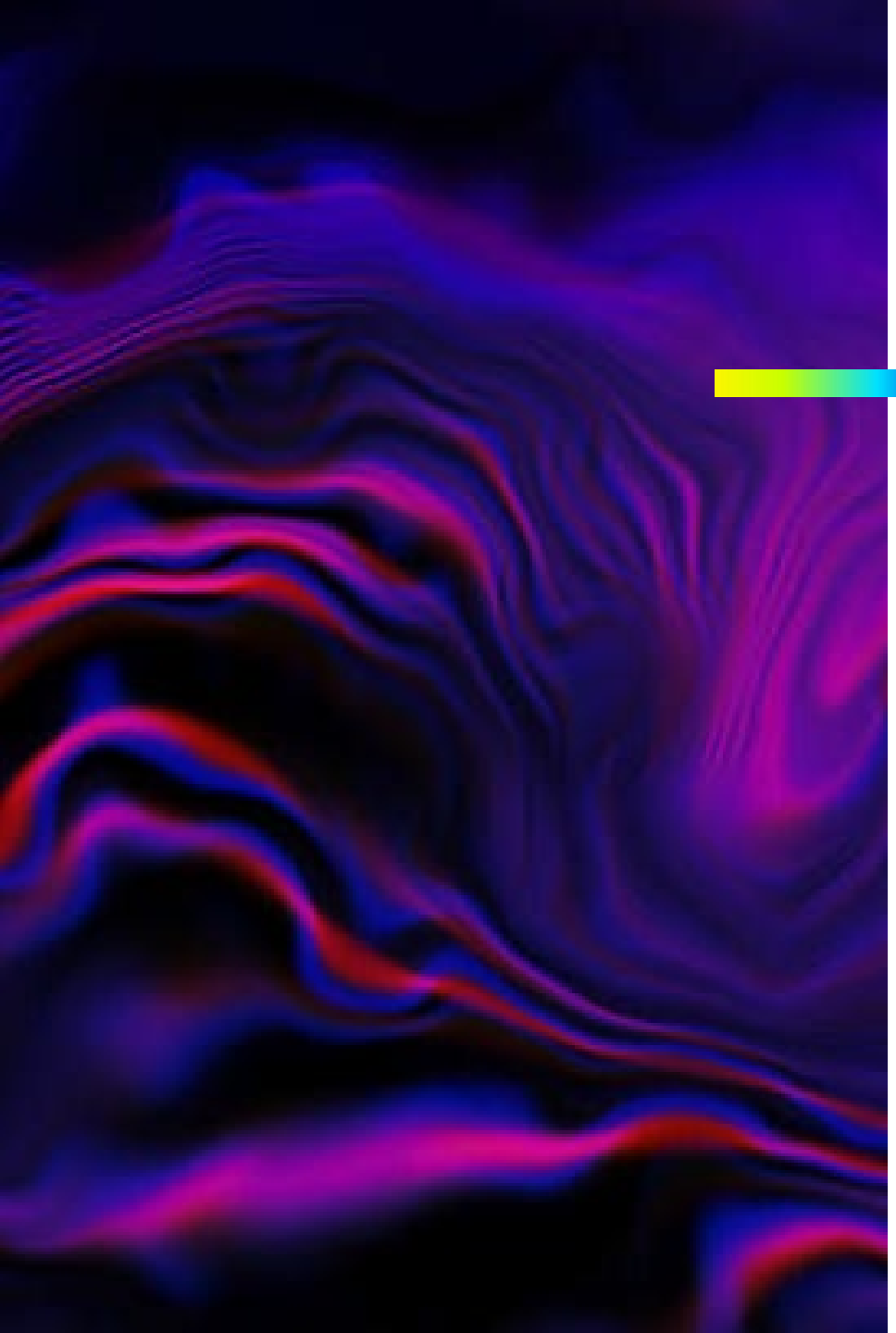


AUSBREITUNG UND RECHTEERWEITERUNG: EXPLORATIVER ANSATZ

Alternativer Untersuchungsansatz
Prüfung der `intra.lan` Domäne auf ausnutzbare Schwachstellen:

- **Kritische Sicherheitslücke**
  Domänen-Administrator-Zugangsdaten in GPO der `intra.lan` enthalten
- Kann von jedem Angreifer mit Domänen-Zugangsdaten entschlüsselt werden
- Ausnutzung hinterlässt keine Spuren
- Andere Domänen waren nicht betroffen
- weitere Schwachstellen ohne Hinweise auf Ausnutzung
- **GPO = Wahrscheinlichstes Szenario für die Privilege Escalation des Angreifers**





AUSFÜHRUNG DER RANSOMWARE

- `w.exe` nur auf 961 Systemen gezielt platziert und ausgeführt
- Keine Anzeichen für automatisierte Verteilung
- Angreifer definierten Windows-Defender-Ausnahmen um die Erkennung zu Erschweren
- Verschlüsselung der Zielsysteme und anschließend rekursiv der erreichbaren Netzwerkfreigaben
- Dateien werden nur teilverschlüsselt (ca. 10-25%)

04

RISIKOBEWERTUNG → WIEDERHERSTELLUNG

- Backup-Situation
- Persistenz im Netzwerk
- Bewertung Datenabfluss

Reframe your readiness.

BACKUP SITUATION

Erste nachweisbare Angreiferaktivitäten am 18.10.2023

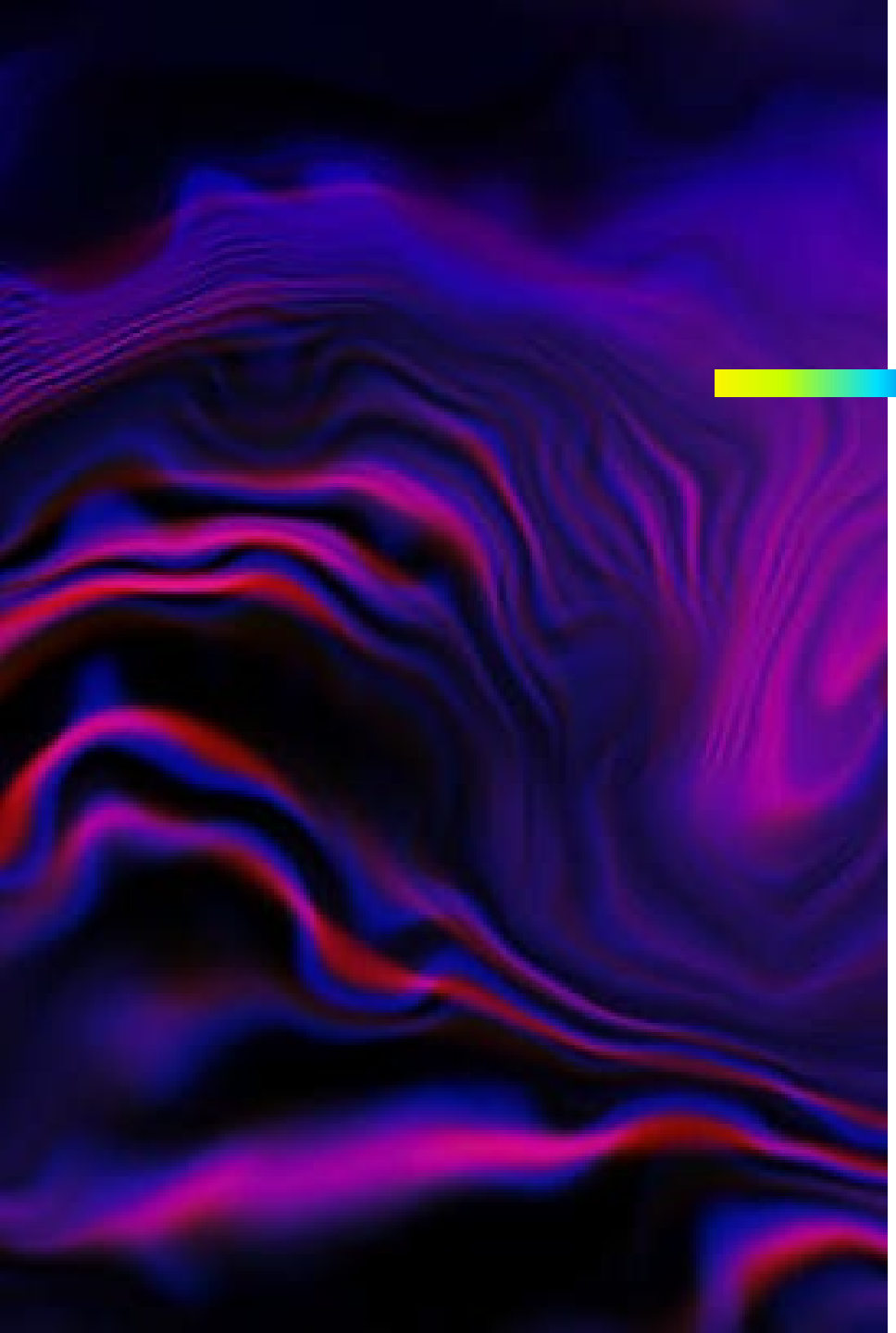
- Hohe Wahrscheinlichkeit, dass Nutzdaten vor dem 18.10.2023 nicht kompromittiert sind

Neuaufbau der Systeme der `intra.lan` Domäne (rote Zone)

- Sehr geringe Wahrscheinlichkeit für die Wiederherstellung von Backdoors oder Sicherheitslücken

Mehrstufiges Scan-/Prüfkonzept für wiederhergestellte Daten

- Zusätzliche Absicherung gegen Artefakte des Angreifers



PERSISTENZ IM NETZWERK

- **Keine Hinweise auf Übersprung aus `intra.lan`**

- kurzfristige implementierte Maßnahmen zielten auf eine verstärkte Überwachung auf neue Angriffsaktivitäten
- Keine Persistenzmechanismen in der `intra.lan` Domäne identifiziert
- Vorhandensein des Angreifers in der Organisation kann zum jetzigen Zeitpunkt mit hoher Wahrscheinlichkeit ausgeschlossen werden

EINSCHÄTZUNG ZUM DATENABFLUSS

- Erfolgloser Nutzungsversuch von WinRAR
- **Keine konkreten Anzeichen für Datenabfluss**
- Kein auffälliger Webverkehr / File-Uploads
- Keine Ankündigung im Blog von Akira
- Keine Hinweise im Darkweb-Monitoring

Jedoch: Keine absolute Gewissheit.
Eine Veröffentlichung bleibt möglich,
wird aber für unwahrscheinlich gehalten.

05

VERBESSERUNGS-MAßNAHMEN

- Implementierte und geplante Maßnahmen

Reframe your readiness.

IMPLEMENTIERTE UND GEPLANTE MAßNAHMEN

KURZFRISTIG (UMGESETZT)

- Forensik-Scan
- Wiederherstellung aus Backup
- Netzwerksegmentierung
- Next-Generation-Firewall
- **Best Practices Systemhärtung**
- **Absicherung Benutzerkonten**
- Endpoint Detection and Response
- Protokollierung
- **Absicherung VPN + MFA**
- Darkweb Monitoring

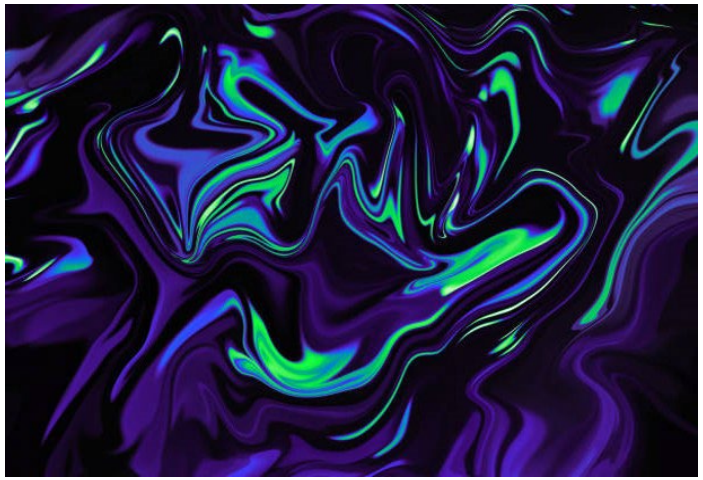
MITTELFRISTIG (IN UMSETZUNG ODER IN PLANUNG)

- Mikrosegmentierung
- SSL-Interception
- Erweiterte Systemhärtung
- Erweiterte Kontenabsicherung
- Erweiterung der EDR-Module
- Next-Generation-SIEM-System
- **Schwachstellen-Management**
- Fortgesetztes Darkweb Monitoring

LANGFRISTIG

- Cyber-Security-Plan
- Hybride Absicherung Web Access
- Strategisches IAM: RBA, Tiering, PAM, SSO
- **Penetrationstestpläne / Red Teaming**

FRAGEN



Marek Stiefenhofer

Geschäftsführender Gesellschafter

Hatzfelder Str. 167
D-42281 Wuppertal

Telefon: +49 202 31767-100
E-Mail: info@r-tec.net
www.r-tec.net

Südwestfalen-IT Sonnenblumenallee 3 58675 Hemer

An alle HVB im Verbandsgebiet

Auskunft erteilt: Jörg Kowalke
Durchwahl: +49 271 30 321-1279
E-Mail: joerg.kowalke@sit.nrw
Aktenzeichen: Entgelte2024

Datum: 18.01.2024

Cyberangriff auf die Südwestfalen-IT –
Zahlung der Entgelte 2024

Sehr geehrte Damen und Herren,

zuletzt haben wir mit Schreiben vom 09.01.2024 darum gebeten, die Entgelte für 2023 vollständig zu begleichen, um die Handlungsfähigkeit des Zweckverbands zu sichern. In der Vorstandssitzung vom 17.01.2024 wurde darüber beraten, wie mit der Rechnungsstellung und Zahlung der Entgelte für 2024 verfahren werden soll. Aufgrund der weiterhin sehr angespannten Liquiditätslage, sind die Vorstandsmitglieder zu dem einstimmigen Votum gekommen, dass die Entgelte 2024 zu 100% berechnet und bezahlt werden sollen, um die Handlungsfähigkeit des Zweckverbandes zu gewährleisten. Dies gilt unabhängig davon, ob eine Leistung ganz oder teilweise nicht erbracht werden kann. Eine finale Entscheidung zum Umgang mit den Abrechnungen und ggf. Erhebung einer Verlustumlage für 2024 soll noch in diesem Jahr in den Gremien getroffen werden.

Aus diesem Grund möchten wir Sie höflich bitten, die anstehenden Entgeltrechnungen betreffend das Jahr 2024 termingerecht anzuweisen. Verbandsvorsteher und Geschäftsführung versichern Ihnen, dass jetzt geleistete Zahlungen unter dem Vorbehalt einer finalen Klärung der Modalitäten für die Entgeltzahlungen 2024 stehen. Sobald die Gremien dazu Beschlüsse gefasst haben, werden die Rechnungen für alle Verbandsmitglieder korrigiert und etwaige Überzahlungen verrechnet oder erstattet. Im Ergebnis werden keinem Verbandsmitglied, das jetzt durch seine Entgeltzahlung den Zweckverband in seiner Handlungsfähigkeit unterstützt, aus diesem Handeln Nachteile bei der späteren Klärung der finanziellen Abwicklung des Jahres 2024 entstehen.

Wir hoffen, Ihnen mit dieser Zusage eine ausreichende Sicherheit für das Anweisen ggf. vorliegender Rechnungen zu geben und bedanken uns schon jetzt für das kooperative Vorgehen.

Für Rückfragen steht Ihnen die Geschäftsführung gerne zur Verfügung.

Mit freundlichen Grüßen

Theo Melcher
- Verbandsvorsteher -

Jörg Kowalke
- stv. Geschäftsführer -