

Angriff auf die SIT

Bericht zum Ablauf

Veranstaltung „Kommunal sicher“
am 25.06.2024



Jörg Kowalke

18.06.2024

1.0

01

Erläuterung
Abschlussbericht

02

Aktuelle
Wiederanlaufplanung

03

Ausblick

01 Erläuterung Abschlussbericht



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

01 Erläuterung Abschlussbericht



30.10.2023, 14:00

- 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



30.10.2023, 11:00 – 12:00

- Gemeinsame Konferenz zur Abstimmung des weiteren Vorgehens



01 Erläuterung Abschlussbericht



Erster Zugang 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 SIT 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 auf diese Schwachstelle in Kombination mit fehlender MFA „spezialisiert“
- „Lateral Movement“ begünstigt durch GPO/Admin



Systeme herunterfahren

Um eine eventuelle Ausbreitung zu verhindern wurden sämtliche Systeme heruntergefahren



Informationen an Kunden, Partner und Presse

Aufgrund der Abschottung wurden Informationen auf dem Postweg und über externe E-Mailadressen verteilt



r-tec und Krisenstab

Einberufen von Experten zur Schadensbegrenzung und Problemlösung



Wiederaufbauprojekt

Mit der Unterstützung unserer Mitglieder und befreundeter Rechenzentren konnte der Wiederaufbau begonnen werden

Zeitplanung/Fortschrittsanzeige – Prio 1



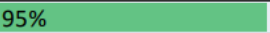








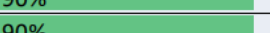






Fachverfahren	Nutzer	Betreiber	Basisbetrieb	Phase 1	Normalbetrieb	Status Funktionalität*
KDN.Sozial	Nord+Externe	SIT	Live	Live	Live	100%
Inforegister	Nord+Externe	SIT	Live	Live	Live	95%
VOIS MESO	Nord+Externe	SIT	Live	Live	KW 26 (21)	95%
ADVIS	Nord+Süd+Externe	SIT	Live	Live	KW 27 (23)	95%
OK.Verkehr	Nord+Süd	regio iT	Live	Live	KW 26 (25)	99%
OK.EWO	Süd	SIT	Live	Live	KW 31 (24)	95%
Autista/ePR	Nord+Süd+Externe	SIT	Live	Live	Live	100%
Infoma	Nord+Süd+Externe	SIT	Live	Live	KW 26 (24)	95%
MACH	Nord+Extern	SIT	Live	Live	Live	100%
WG Plus	Nord+Externe	SIT	Live	./.	Live	100%
CZ Wohngeld	Süd	regio iT	Live	./.	Live	100%



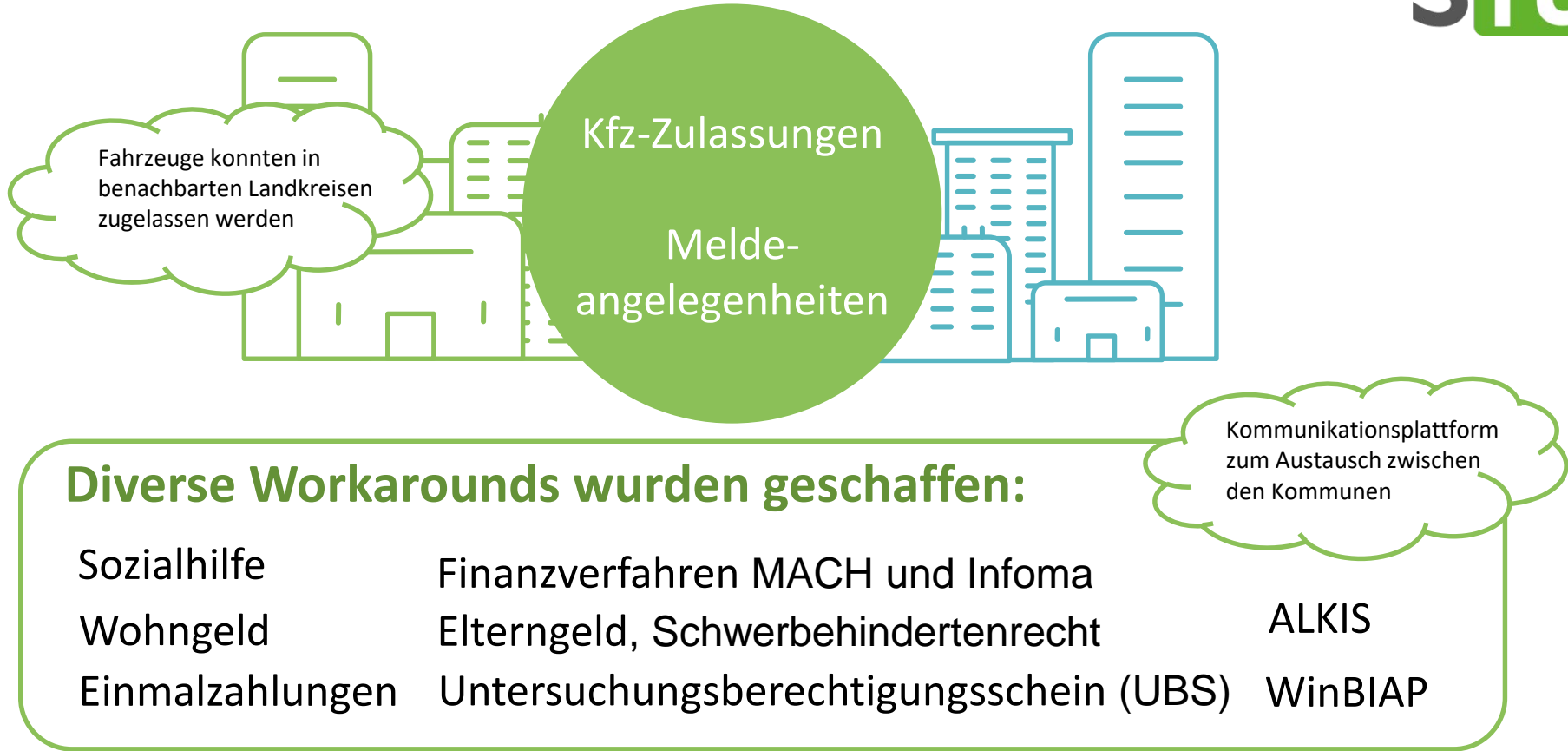
Phase 1 => erste Erweiterung Funktionsumfang / Schnittstellen

Zeitplanung/Fortschrittsanzeige – Prio 2 & 3



Verfahren	Info	Nutzer	Betreiber	Basisbetrieb	Normalbetrieb	Status Funktionalität*
SD.NET	Abstimmung mit KDVB Frechen	Süd	KDVZ	Live	KW 35 (26)	95% 
SC-OWI	Wiederanlauf	Nord	SIT	Live	Live	100% 
WinOWIG	Neuaufbau	Nord & Süd	SIT	Live	Live	100% 
VoteManager	Auslagerung zur KDVB Frechen	Nord & Süd	KDVZ	Live	Live	90% 
ProSozBau (ProBauG)	Neuaufbau	Süd	SIT	Live	Live	90% 
ALKIS	Neuaufbau	Süd	SIT	Live	Live	100% 
beBpo	Wiederanlauf	Nord & Süd	SIT	Live	Rollout	99% 
citkoPortal / Form-Solutions	Nur Serveranlauf, Betrieb durch nextgov iT	Nord & Süd	SIT / nextgov iT	Live	Live	95% 
Doxis	Wiederanlauf	Nord	SIT	Live	KW 25 (24)	90% 
Enaio	Neuaufbau	Süd	SIT	Live	KW 25 (24)	90% 
Loga	Extern krz, bereits lauffähig	Nord & Süd	OWL-IT	Live	Live	100% 
Migewa	Auslaufbetrieb wg. Migration VOIS GESO	Süd	SIT	Live	KW 27 (24)	60% 
WinBIAP	Wiederanlauf	Nord & Süd	SIT	Live	Live	95% 
VOIS GESO	Wiederanlauf	Nord	SIT	Live	Live	95% 
Vollstreckung Infoma	Neuaufbau	Nord & Süd	SIT	./.	Live	100% 
WinFried	Neuaufbau	Süd	SIT	im Rollout	im Rollout	60% 

Amtshilfe - Städte helfen Städten



Fahrzeuge konnten in benachbarten Landkreisen zugelassen werden

Kfz-Zulassungen

Melde-angelegenheiten

Diverse Workarounds wurden geschaffen:

Sozialhilfe

Finanzverfahren MACH und Infoma

Wohngeld

Elterngeld, Schwerbehindertenrecht

Einmalzahlungen

Untersuchungsberechtigungsschein (UBS)

ALKIS

WinBIAP

Kommunikationsplattform zum Austausch zwischen den Kommunen

03 Ausblick



- Nutzen Zweckverband / Zentralisierung / Standardisierung
 - Nutzen von Zentralisierung
 - Skaleneffekte realisieren
 - Kommunale IT ist komplex
 - überfordert viele der kleinen und mittleren Kommunen
 - Fachkräftemangel



Implementierte und geplante Maßnahmen



Kurzfristig (Umgesetzt)

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

Mittelfristig (in Umsetzung oder Planung)

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

Statistiken

Anzahl der Schwachstellen und Schadsoftware



Mehr als **2000** Schwachstellen in Software Produkten (15% davon Kritisch) wurden in einem Berichtszeitraum von einem Monat bekannt. Zuwachs von 24%

Eine Viertelmillion neue Schadprogramm-Varianten wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.

Quelle: BSI Lagebericht 2023

Fragen?

