

Wahlperiode 2020 – 2025

Niederschrift

Über die 14. öffentliche Sitzung des Ausschusses für Finanzen, Bau und Digitalentwicklung vom Donnerstag, den 07.03.2024, Aula Kulturhaus Lyz in Siegen, St.- Johann-Straße 18, 57072 Siegen

<u>Beginn der öffentlichen Sitzung:</u>	17:01 Uhr
<u>Ende der öffentlichen Sitzung:</u>	17:59 Uhr
<u>Beginn der nichtöffentlichen Sitzung:</u>	17:59 Uhr
<u>Ende der nichtöffentlichen Sitzung</u>	18:10 Uhr

Anwesenheitsliste

Vorsitz

Bernd-Dieter Ferger

stimmberechtigte Mitglieder

Helmut Kaufmann für: Tim Lukas Debus
Max Hennes
Heinz-Werner Denker für: Julian Maletz
Michael Franz für: Daniel Stettner
Karl Ludwig Völkel
Martin Achatzi für: Prof. Martin Ferger
R. Wettlauber für: Volker Schwarz
Thomas Helmkampf
Axel Boldt
Joachim Boller für: Ulrich Schmidt-Kalteich
Sven Hendrik Schütz
Sven Kellert für: Ursula Regine Stephan
Wolfgang Decker
Hans Peter Kunz
Ulrich-Eberhardt Georgi
Gerd Groß

entschuldigte Mitglieder

Tim Lukas Debus
Julian Maletz
Daniel Stettner
Prof. Martin Ferger
Volker Schwarz
Ulrich Schmidt-Kalteich
Ursula Regine Stephan
Sebastian Zimmermann

Gäste/Zuhörer

1 Vertreter der Presse
Mirco Pinske, Geschäftsführer SIT

Jörg Kowalke, stellv. Geschäftsführer SIT

Verwaltung

Tobias Wein, Dezernent I

Arno Wied, Dezernent IV

Thomas Wüst, Dezernent III

Jürgen Heine, Amtsleiter Amt für Finanzwirtschaft

Benedikt Schneider, Stv. Amtsleiter Amt für Finanzwirtschaft/Schriftführer

Henning Schneider, Amtsleiter Personalamt

Michael Haßler, Amtsleiter Amt für Immobilien

Tagesordnung

Öffentliche Sitzung

1. Bericht der Verwaltung
2. Anfragen
 - 2.1 Folgen des Cyber-Angriffs auf die Südwestfalen-IT
Anfrage der Fraktion Die Linke
Drucksache 3/2024
 - 2.1.1 Folgen des Cyber-Angriffs auf die Südwestfalen-IT
Beantwortung der Anfrage der Fraktion Die Linke
Drucksache 3/2024 1. Ergänzung
 - 2.2 Sicherheit der SIT GmbH
Anfrage der Fraktion Bündnis 90/Die Grünen
Drucksache 56/2024
 - 2.2.1 Sicherheit der SIT GmbH
Beantwortung der Anfrage der Fraktion Bündnis 90/Die Grünen
Drucksache 56/2024 1. Ergänzung
3. Tagesordnungspunkte nur für den Ausschuss
 - 3.1 Bericht Cyber-Angriff; Mündlicher Bericht des stv. Geschäftsführers der Südwestfalen-IT (SIT) Jörg Kowalke
Mündlicher Bericht
 - 3.2 Übersicht der Baumaßnahmen des 2023 und deren Kostenentwicklung
Drucksache 33/2024
 - 3.3 Übersicht über geplante Ermächtigungsübertragungen gem. § 22 KomHVO ab 50.000.- Euro von 2023 nach 2024
Drucksache 37/2024
 - 3.4 Übersicht der projektbezogenen Stellen des Kreises Siegen-Wittgenstein

Drucksache 44/2024

4. Tagesordnungspunkte für Kreisausschuss und/oder Kreistag
 - 4.1 Stundung, Niederschlagung, Erlass von Forderungen des Kreises Siegen-Wittgenstein; Kenntnisnahme von Entscheidungen, die der Landrat aufgrund der veränderten Beträge in § 15 der Hauptsatzung getroffen hat
Drucksache 36/2024
5. Anträge gem. § 2 Abs. 1 der Geschäftsordnung
6. Verschiedenes

Sitzungsverlauf

Der Ausschussvorsitzende **Herr Bernd Dieter-Ferger** eröffnet um 17:01 Uhr die Sitzung und begrüßt alle Ausschussmitglieder sowie die Vertreter der Presse und der Verwaltung. Weiter begrüßt Herr Ferger die eingeladenen Vertreter der Südwestfalen-IT, Herrn Pinske (Geschäftsführer der Südwestfalen-IT) und Herrn Kowalke (stellv. Geschäftsführer der Südwestfalen-IT).

Herr **Ferger** begrüßt zudem das neue Ausschussmitglied, Herrn Sven Kellert. Herr Ferger erklärt, dass vor Beginn der Sitzung die Verpflichtung von Herrn Kellert als neues Ausschussmitglied erfolgen muss. Er bittet alle Anwesenden sich von den Plätzen zu erheben und verliest die Verpflichtungsformel.

1. Bericht der Verwaltung

Beratungsverlauf:

Ein Bericht der Verwaltung liegt nicht vor.

2. Anfragen

Beratungsverlauf:

Es liegen keine Anfragen vor.

- 2.1 Folgen des Cyber-Angriffs auf die Südwestfalen-IT
Anfrage der Fraktion Die Linke
Drucksache 3/2024

- 2.1.1 Folgen des Cyber-Angriffs auf die Südwestfalen-IT
Beantwortung der Anfrage der Fraktion Die Linke
Drucksache 3/2024 1. Ergänzung

Beratungsverlauf:

Herr **Georgi** hat eine ergänzende Frage zu Beantwortung der Anfrage. Er merkt an, dass in dem Schreiben von Abschlagszahlungen gesprochen wird. Er möchte wissen, wie hoch diese sind.

Herr **Wein** erklärt, dass Rechtsansprüche von Kunden erfüllt werden müssen. Ihm seien keine Rechtsstreitigkeiten bezüglich der Forderungen bekannt. Man habe Auszahlungen geleistet, damit bei der SIT weitergearbeitet werden konnte. Man müsse gegebenenfalls später nachbessern.

2.2 Sicherheit der SIT GmbH
Anfrage der Fraktion Bündnis 90/Die Grünen
Drucksache 56/2024

2.2.1 Sicherheit der SIT GmbH
Beantwortung der Anfrage der Fraktion Bündnis 90/Die Grünen
Drucksache 56/2024 1. Ergänzung

Beratungsverlauf:

Herr **Schütz** möchte wissen, wer bei der SIT wem berichtspflichtig war und wer der Sicherheitsbeauftragte bei der SIT zu dem Zeitpunkt war.

Herr **Wein** weist daraufhin, dass es sich bei dem Cyberangriff um einen hochprofessionellen und ressourceneinsatzstarken Angriff einer weltbekannten Cybercrimegruppe gehandelt hat. Er kann verstehen, dass im Nachhinein Fehler erkannt werden und diese auch angesprochen werden. Er kann den Umgang mit der Angelegenheit nicht ganz nachvollziehen. Aus seiner Sicht soll ein Schuldiger gefunden werden, der für die Versäumnisse die Verantwortung übernehmen soll.

Er bittet darum, zunächst den später folgenden Vortrag von Herrn Kowalke abzuwarten. Möglicherweise würden dann manche Sachverhalte neu eingeordnet. Herr Wein erklärt weiter, dass es sich bei der SIT um einen Zweckverband handelt, in dem der Kreis Siegen-Wittgenstein ein Mitglied ist. Man habe die Fragen so weit wie möglich beantwortet, es könne jedoch nicht alles in der Öffentlichkeit dargestellt werden.

Er verweist zudem auf den forensischen Bericht.

Herr **Ferger** meint, dass man glücklich sein könne heute einen mündlichen Bericht von den Vertretern der SIT zu bekommen. Er bittet Herrn Kowalke um einen realistischen, neutralen und verständlichen Vortrag. Er bittet insbesondere darum, auf Fachbegriffe zu verzichten.

3. Tagesordnungspunkte nur für den Ausschuss

3.1 Bericht Cyber-Angriff; Mündlicher Bericht des stv. Geschäftsführers der Südwestfalen-IT (SIT) Jörg Kowalke
Mündlicher Bericht

Beratungsverlauf:

Herr **Kowalke** berichtet über den zeitlichen Ablauf des Cyberangriffs. Er gibt dabei Erläuterung zu dem möglichen Vorgehen der Angreifer und erklärt, wie zukünftig vorbeugende Maßnahmen aussehen könnten. Die bei dem Vortrag verwendete Powerpoint-Präsentation ist dem Protokoll als Anlage beigefügt.

Herr **Ferger** bedankt sich für die sachliche Darstellung bei Herrn Kowalke.

Herr **Kunz** bedankt sich bei Herrn Kowalke für den Vortrag. Er hat jedoch eine Anmerkung zu dem Abschlussbericht über den Cyberangriff. Er kritisiert diesbezüglich die Verwaltung, da der Bericht nicht an die Fraktion übermittelt wurde und dieser auch nicht auf der Seite der

Kreisverwaltung zu finden war. Öffentlich zugänglich sei der Abschlussbericht aus seiner Sicht nicht gewesen.

Herr **Kunz** hat aus dem Vortrag von Herrn Kowalke entnommen, dass der Angriff mutmaßlich nach Brute-Force Methode erfolgt ist. Dabei wurde eine Schwachstelle bei Cisco-Systems ausgenutzt. Das System akzeptierte mehr als drei fehlerhafte Anmeldeversuche. Er habe aus der Presse entnommen, dass diese Sicherheitslücke länger bekannt war und es hierfür ein Sicherheitspatch gab. Er möchte wissen, seit wann dies bekannt war und warum der Sicherheitspatch nicht eingespielt wurde. Zudem möchte Herr Kunz wissen, ob die Stellen der Sicherheitsorganisation bei der SIT zum Zeitpunkt des Cyberangriffes alle besetzt waren.

Herr **Kowalke** merkt zunächst an, dass er zu dem Sicherheitssystem der SIT in der Öffentlichkeit keine Angaben machen möchte. Die im Antwortschreiben der Anfrage aufgeführten Stellen seien aber alle besetzt gewesen. Bezüglich des Sicherheitspatches sagt Herr Kowalke, dass dies Thema der Aufarbeitung sei.

Herr **Achatzi** hat 3 Fragen an Herrn Kowalke, die in der Sitzung nicht abschließend beantwortet werden konnten. Diese sollen dem Protokoll beigelegt werden.

Die schriftliche Beantwortung der Fragen ist im Protokoll des nichtöffentlichen Teils unter Punkt 6, Verschiedenes, eingefügt worden, da es sich um interne Informationen handelt, die in der Öffentlichkeit nicht dargestellt werden sollten.

Herr **Ferger** bedankt sich nach Abschluss der Diskussion nochmals bei Herrn Kowalke und Herrn Pinske für den mündlichen Vortrag und ihr Erscheinen.

3.2 Übersicht der Baumaßnahmen des 2023 und deren Kostenentwicklung **Drucksache 33/2024**

Beratungsverlauf:

Es findet keine Beratung statt.

3.3 Übersicht über geplante Ermächtigungsübertragungen gem. § 22 KomHVO ab 50.000.- Euro von 2023 nach 2024 **Drucksache 37/2024**

Beratungsverlauf:

Es findet keine Beratung statt.

Abstimmungsergebnis:

Zur Kenntnis genommen

3.4 Übersicht der projektbezogenen Stellen des Kreises Siegen-Wittgenstein **Drucksache 44/2024**

Beratungsverlauf:

Verschiedene Ausschussmitglieder merken an, dass ihnen die Vorlage nicht zugesandt wurde.

Herr **Ferger** meint, dass unter diesen Umständen der TOP in die nächste Sitzung des Finanzausschuss verschoben werden soll und die Vorlage dann allen Ausschussmitgliedern vorliegt.

Herr **Achatzi** möchte noch wissen, ob mit Auslaufen des Förderprogramms Klimaresilienz am 29.02.2024 eine zusätzliche Stelle verbunden war und wenn ja, ob diese weitergeführt worden ist.

Die Beantwortung der Frage soll in der nächsten Sitzung des Finanzausschusses erfolgen, wenn allen Ausschussmitgliedern die Unterlagen vorliegen.

4. Tagesordnungspunkte für Kreisausschuss und/oder Kreistag

4.1 Stundung, Niederschlagung, Erlass von Forderungen des Kreises Siegen-Wittgenstein; Kenntnisnahme von Entscheidungen, die der Landrat aufgrund der veränderten Beträge in § 15 der Hauptsatzung getroffen hat
Drucksache 36/2024

Beratungsverlauf:

Herr **Helmkamp** hat eine Anmerkung zu der Vorlage. In der Sachdarstellung werde auf eine Änderung der Hauptsatzung aus 2004 hingewiesen. Er möchte wissen, ob dieser Hinweis noch erforderlich sei.

Dies wird durch die Geschäftsführung des Ausschusses geprüft.

5. Anträge gem. § 2 Abs. 1 der Geschäftsordnung

Beratungsverlauf:

Es liegen keine Anträge vor.

6. Verschiedenes

Beratungsverlauf:

Es findet keine Beratung statt.

Herr Ferger schließt um 17:59 Uhr die öffentliche Sitzung.

Ausschussvorsitzender

Schriftführer

Bernd-Dieter Ferger

Benedikt Schneider

Cyberangriff SIT Bericht und Ausblick

Sitzung aus Digitalisierungsausschusses am 07.03.2024



Jörg Kowalke

29.02.2024

1.01

Anlage

Agenda

01
Erläuterung
Abschlussbericht

02
Aktuelle
Wiederanlaufplanung

03
Ausblick

01 Erläuterung Abschlussbericht



01 Erläuterung Abschlussbericht



30.10.2023, 11:00 – 12:00

- Gemeinsame Konferenz zur Abstimmung des weiteren Vorgehens



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

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

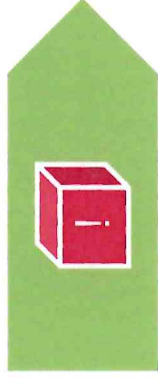
Ungeklärte Beschaffung der Zugangsdaten

- 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

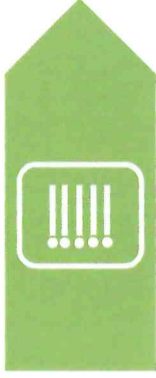
- Es gab Anzeichen für vermehrte Anmeldeversuche vor dem Angriff
- Cisco ASA Schwachstelle CVE-2023-20269 erleichtert Brute-Forcing
- S-IT war von der Schwachstelle betroffen
- Akira hat sich auf diese Schwachstelle in Kombination mit fehlender MFA „spezialisiert“

Maßnahmen



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

02 Aktuelle Wiederanlaufplanung



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

Phase 1 => erste Erweiterung Funktionsumfang / Schnittstellen

Fachverfahren Priorität 2/3



Verfahren	Info	Nutzer	Betreiber	Basis- betrieb	Normal- betrieb
SD.NET	Abstimmung mit KDZV Frechen	Süd	KDVZ	KW 10	KW 14
SC-OWI	Wiederanlauf	Nord	SIT	Live	KW 14
WinOWIG	Neuaufbau	Nord & Süd	SIT	KW 08 (07)	KW 10 (14)
VoteManager	Auslagerung zur KDZV Frechen	Nord & Süd	KDVZ	Live	Live
ProSozBau (ProBauG)	Neuaufbau	Süd	SIT	Live	KW 13
ALKIS	Neuaufbau	Süd	SIT	KW 13	KW 22
beBPO	Wiederanlauf	Nord & Süd	SIT	Live	Rollout
citkoPortal / Form- Solutions	Nur Serveranlauf, Betrieb durch nextgov iT	Nord & Süd	SIT / nextgov iT	KW 09	KW 10
Doxis	Wiederanlauf	Nord	SIT	KW 09	KW 18
Enaio	Neuaufbau	Süd	SIT	KW 09	KW 18
Loga	Extern krz, bereits lauffähig	Nord & Süd	OWL-IT	Live	Live
Migewa	Auslaufbetrieb wg. Migration VOIS GESO	Süd	SIT	KW 14	KW 18
WinBIAP	Wiederanlauf	Nord & Süd	SIT	KW 10 (14)	KW 18
VOIS GESO	Wiederanlauf	Nord	SIT	Live	KW 18
Vollstreckung Infoma	Neuaufbau	Nord & Süd	SIT	KW 13	KW 16

Infrastruktur Priorität 2/3

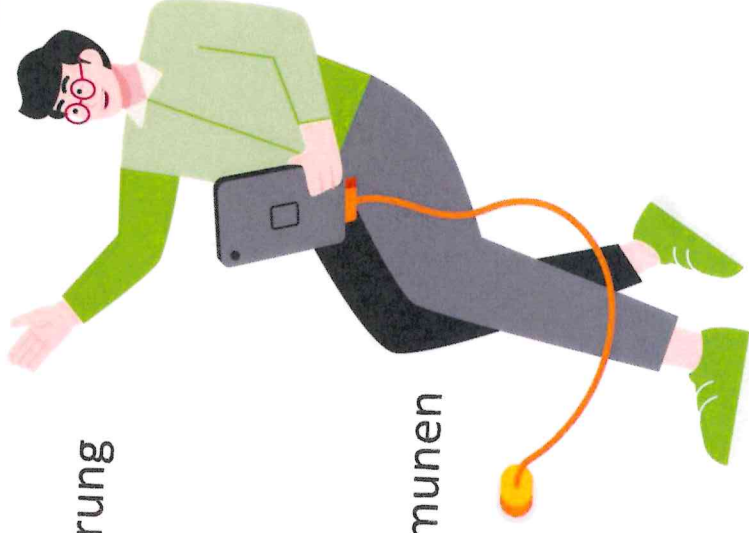


Verfahren	Info	Nutzer	Betreiber	Basis- betrieb	Normal- betrieb
Transfer CI	Wiederanlauf	Nord & Süd	SIT	Live	Live
UC4	Wiederanlauf	Nord & Süd	SIT	Live	Live
Client VPN	Neuaufbau	Nord & Süd	SIT	./.	KW 13
Active Sync Nord	Wiederanlauf	Nord	SIT	./.	Live
V-PKI	Wiederanlauf	Nord & Süd & Ex	SIT	./.	KW 09 (05)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

03 Ausblick

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

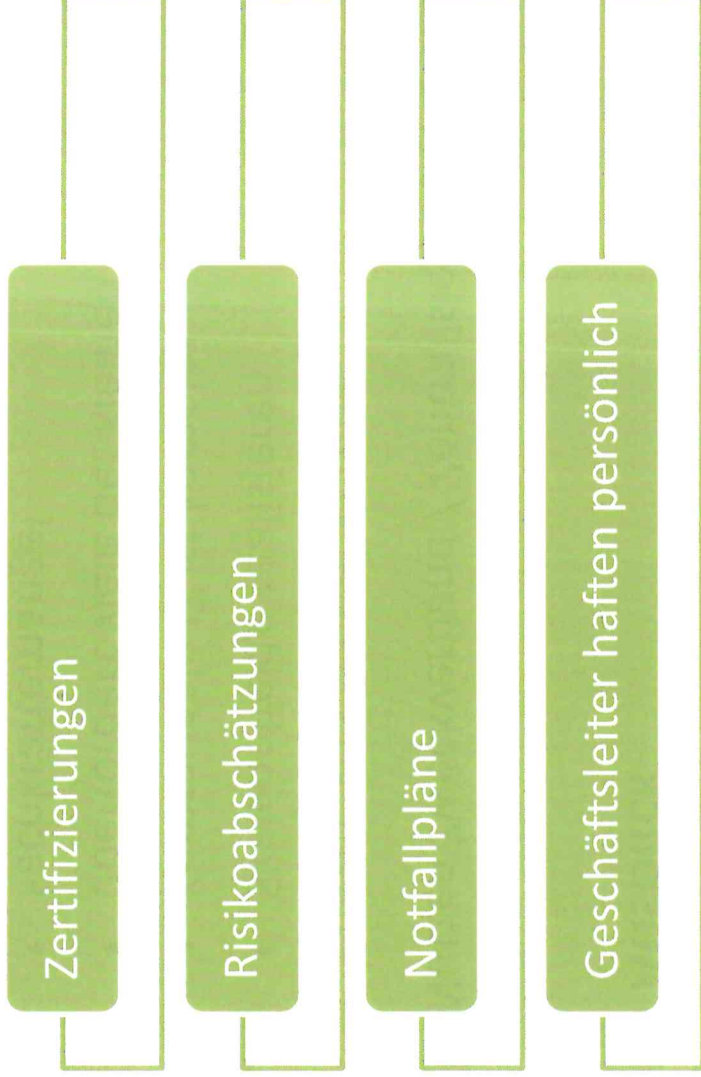
sit



NIS2



Hohe Anforderungen an die Dienstleister



Anwendung auf komm. IT-Dienstleister zzt. Umstritten

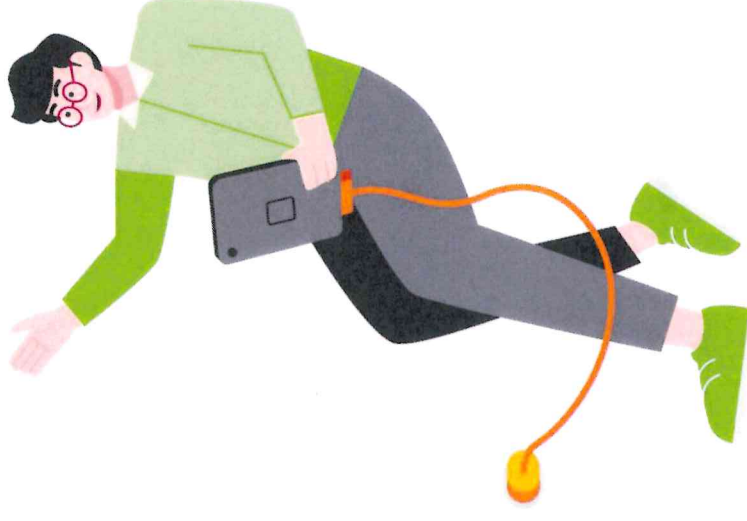
IT-PLR hat Anfang November gegen Anwendung plädiert

Ausgang zzt. noch offen, finale Gesetzgebung in Q4/2024 zu erwarten

Aufstellung der SIT für die Zukunft

- Reform-Prozess in NRW ist angeteasert
- aktuell ca. 35 kommunale IT-Dienstleister
- Gutachten der komm. Spitzenverbände
 - Ziel: ein zentraler IT-Dienstleister in NRW
 - Sukzessiver Beitritt von Kommunen und IT-Dienstleistern freiwillig vorgesehen
- Konsolidierung sinnvoll und notwendig
- Beispiel Ressourcen für IT-Sicherheit

SIT



Fragen?

