

Der Weg in die Basis-Absicherung (WiBA) am Beispiel der Modellkommune Markleeberg



Die Lage

Durchschnitt

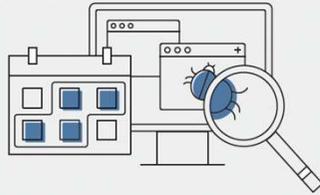
Gesellschaft



Identitätsdiebstahl

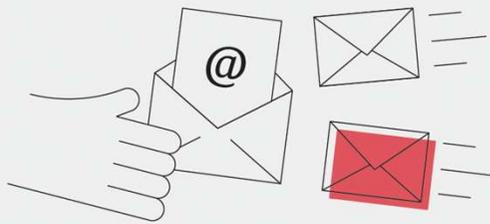
Sextortion
Phishing

— Täglicher Zuw 32 % Be



Rund **21.000** infizierte Systeme wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** E-Mails mit Schadprogrammen wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.



370 Webseiten wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.



Abhängigkeit von IT-gestützten Verfahren ist groß

Cyberangriffe nehmen zu und werden professioneller

Keine Frage ob man betroffen sein wird, sondern wann?

Quelle: Bericht zur Lage der IT-Sicherheit in Deutschland 2023, Bundesamt für Sicherheit in der Informationstechnik

Der Weg in die Basis-Absicherung (WiBA)

Die Idee

Der Lösungsansatz

Die Beteiligung

Weg in die Basis-Absicherung (WiBA)

Die Idee



Einstieg in den BSI
IT-Grundschutz trotz Basis-
Absicherung teilweise zu
komplex

vielen kleinen Institutionen
fehlen ausreichend
Ressourcen und Know-How

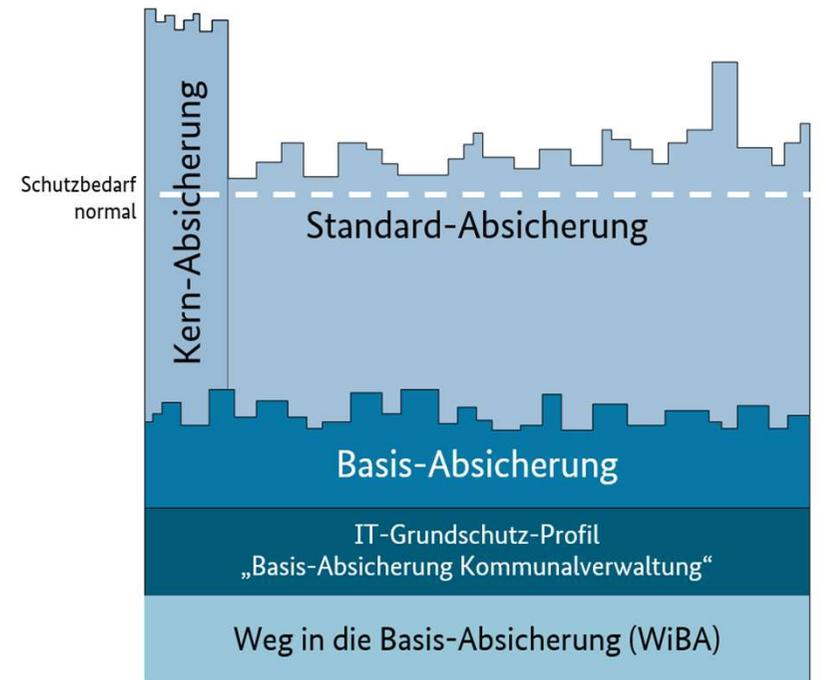
Im Fokus: **Kommunen**

Der Lösungsansatz

Ziel -> **Sachstände erhoben** und umzusetzende **Anforderungen mittels Prüffragen** und Checklisten mit wenig Aufwänden identifizieren.

Grundlage -> **IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“**

- **WiBA** ist **KEIN** Standard für Informationssicherheit
- Keine Vorkenntnisse zur Methodik des IT-Grundschutzes notwendig
- Es werden **Hilfsmittel** bereitgestellt, die bei der **Umsetzung** unterstützen.



Die Beteiligung

- Einbindung der **Arbeitsgruppe kommunale Basis-Absicherung** (AG koBA) – federführend für das IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“
- Einbindung von **6 Modellkommunen**
 - **Bewerbungs- und Auswahlverfahren** über/mit Kommunalen Spitzenverbänden (DLT, DST, DStGB): über 130 Bewerbungen aus dem Bundesgebiet
 - zwei sehr kleine Kommunen, zwei mittelgroße Kommunen, eine große Stadt, ein Landkreis
 - jeweils **mehrtägige Workshops** Mai und Juni: positives Feedback
 - **Praxiswünsche**: Konkretere Hilfsmittel, Webanwendung zur direkten Bearbeitung der Checklisten, Bereitstellung einer Migrationshilfe zum IT-Grundschutz-Profil „Basis-Absicherung Kommunalverwaltung“
- Community Draft-Phase



Die Modellkommune Stadtverwaltung Marktleeburg

Der Ablauf
Die Effekte

Weg in die Basis-Absicherung (WiBA)

Die Modellkommune Markkleeberg

- 140 Mitarbeitende in der Kernverwaltung, 48 Fachanwendungen, mehr als 30 Server
- Eigene IT-Abteilung mit 5 VZÄ
- Kein KRITIS
- Problem: Grundschutzeinstieg zu komplex, **kein Know-How**, keine Ressourcen
- Größte Schwachstelle: **Dokumentation**
- **Kein BfiS**



Der Ablauf

- WIBA besteht aus 19 Checklisten, Management Summary und Vorgehensanleitung
- nicht nur reine IT-Themen
- **Kernverwaltung** im Fokus
- **Keine Fachanwendungen**
- Mehrfachanwendung möglich und oft nötig
- Priorisierung und Umsetzung

Checkliste	Reihenfolge
Organisation und Personal	1
Rollen / Berechtigungen / Authentisierung	1
Vorbereitung für Sicherheitsvorfälle	1
Backup	1
IT-Administration	2
Client	2
Sicherheitsmechanismen	2
Bürosoftware	2
Netze	2
Serversysteme	2
Serverraum	2
Arbeit innerhalb der Institution / Haustechnik	3
Arbeit außerhalb der Institution	3
Mobile Endgeräte	3
Outsourcing und Cloud	3
Umgang mit Informationen	3
Drucker/Multifunktionsgeräte	4
Telefonie und Fax	4

Der Ablauf

- immer gleicher Aufbau der Checklisten
- mittels Prüffragen, Sachstände zur Informationssicherheit erheben
- umzusetzende Anforderungen identifizieren
- Dokumentation

Arbei Ziel

Prüf Diese Checkliste beschreibt Rahmenbedingungen für das Arbeiten außerhalb der Institution. Dazu gehören neben Telearbeit und damit verbundenem häuslichem Arbeitsplatz auch mobile Arbeitsplätze. Auch Personen, die nicht direkt der Kernverwaltung zuzuordnen sind, wie beispielsweise Gremienmitglieder, sollten für die nachfolgenden Anforderungen sensibilisiert werden.



Nr.

1

In Umgebungen mit mobilen Arbeitsplätzen, wie beispielsweise in öffentlichen Verkehrsmitteln oder bei Klientinnen und Klienten, kann oft keine sichere IT-Infrastruktur vorausgesetzt werden, wie sie in einer Büroumgebung anzutreffen ist. Auch häusliche Arbeitsplätze bieten oft nicht dieselben Sicherheitsvoraussetzungen wie der Büroarbeitsplatz in der Institution. So ist z. B. der Arbeitsplatz oft auch für Besuch oder Familienangehörige zugänglich. Dienstfahrzeuge müssen ebenfalls diesbezüglich betrachtet werden, da nahezu alle modernen Fahrzeuge über integrierte IT-Komponenten wie Infotainmentsysteme verfügen.

Deshalb müssen Maßnahmen ergriffen werden, mit denen sich ein Sicherheitsniveau erreichen lässt, das zumindest vergleichbar mit dem Arbeitsplatz in der Institution ist.

Kernziel der Checkliste ist daher der Schutz der Informationen der Institution bei der Arbeit außerhalb der Institution.

Der Ablauf

Frage	Backup	außerhalb	innerhalb	BüroSoftware	Client	Drucker	IT-Administration	Mobile Endgeräte	Netze	Orga und Personal	Outsourcing Cloud	Rollen Berechtigung	Serverraum	Serversysteme	Sicherheitsmechanismen	Telefonie Fax	Umgang mit Informationen	Vorbereitung Sicherheitsvorfälle
1	2	2	2	2	1	2	2	2	3	2	3	2	3	2	2	2	2	2
2	2	1	3	1	1	2	2	2	1	1	3	1	3	1	2	1	1	3
3	2	2	2	3	1	2	1	2	2	3	2	2	2	2	1	2	2	2
4	2	2	1	2	2	1	2	1	1	2	2	1	3	2	2	2	2	1
5	2	2	1	1	2	1	1	2	2	2	2	2	2	1	2		2	1
6	2	1	2	2	2	2	1	2	3	2	2	2	2	2	2		2	2
7	2	2	2	2	2		1	2	3	1		2	3	3	2		1	3
8		1		1	3		1	2	2	1		2	1	2	2		1	
9		2		1	1		2	1	2	1		1	2	1	2			
10		2		2	2		2	1	2	1		1	2	2				
11				2	1		2	1	3	2		1	2	1				
12				2	2		2	2	2	1		2		1				
13				2	2		1	2	2	2		3		1				
14				1			2	2	1	2		2		1				
15				1			2	2	2	2		2		1				
16				2			1	2	2	2		2		2				
17				1			2	2	2			3		1				
18				1			1	2	1					1				
19				2			2		1					1				
20				1			2		2					2				
21							2		2					3				
22									1									
23									2									
24									2									
25									3									
26									2									
27									2									
28									3									
229	Themenbereiche																	
	76 nicht erfüllt																	
Aktueller Erfüllungsgrad WiBA				66,80%														

Weg in die Basis-Absicherung (WiBA)

Die Effekte



VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

- IT-Notfallrufnummer:
- Wer meldet?
- Welches IT-System ist betroffen?
Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?
- Wann ist das Ereignis eingetreten?
- Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

- Weitere Arbeit am IT-System einstellen
- Beobachtungen dokumentieren
- Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

Ausblick

Die Weiterentwicklung

Die Weiterentwicklung



Weg in die Basis-Absicherung

- Einarbeitung von Rückmeldungen
 - Checkliste „Webserver und Webanwendungen“
- Finalisierung und Veröffentlichung der Dokumente auf der BSI-Webseite (<https://www.bsi.bund.de/dok/wiba>)
 - Vorgehensweise
 - Management Summary - Aufgaben der Leitungsebene
 - 19 Checklisten, inkl. Hilfsmitteln
 - **Migrationstabellen**
- **Perspektivisch:** Anpassung auf aktualisiertes IT-Grundschutz-Profil 4.0, weitere Hilfsmittel/Vorlagen, Toolunterstützung, ...

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Sebastian Thiele-Weineck

Leiter Digitalisierung und IT
Stadtverwaltung Markkleeberg
thiele@markkleeberg.de

Deutschland
Digital•Sicher•BSI•

