EnBW
Cyber Security

Dienstleistungsportfolio-kommunale Beratung

Anforderungen an die Informationssicherheit
für Behörden und Kommunen.

Inhalt

Grundlagen und Anforderungen

Für Kommunen sind die Gewährleistung von Informationssicherheit und Datenschutz lebenswichtig und eine große Herausforderung. Aus diesem Grund hat das Bundesamt für Sicherheit in der Informationstechnik das IT-Grundschutz-Profil zur Basis-Absicherung der Kommunalverwaltung veröffentlicht. Um die darin geforderten Sicherheitskonzepte in der Praxis einzusetzen, unterstützt die EnBW Cyber Security Behörden und Kommunen bei der Umsetzung Ihrer IT-Sicherheit.

Die Informationssicherheit beruht, wie auch der Datenschutz, sowohl auf technischen als auch organisatorischen Maßnahmen. Als Grundlage muss daher eine ausreichende hohe IT-Sicherheit mit dem Ziel umgesetzt werden, die drei grundlegenden Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität zu gewährleisten.

Neben den typischen IT-Sicherheitsthemen wir Virenschutz, Firewalls oder verschlüsselte Datenträger umfasst die Informationssicherheit auch Aspekte der nicht-digitalen Welt.

Daher müssen Themen wie zum Beispiel papiergebundene Informationen, (Geschäfts-) Prozesse und die Gebäudesicherheit berücksichtigt werden, da diese ebenfalls die zu erfüllenden Schutzziele beeinflussen.

Für die Umsetzung der Informationssicherheit wird fast immer auf den Begriff „Stand der Technik" verwiesen, welcher auch in gesetzlichen Vorgaben als notwendiges Niveau aufgeführt wird. Dieser beruht auf gängigen Standards, Normen sowie technischen Richtlinien wie zum Beispiel:

- ISO 27001
- IT-Grundschutz
- Branchenspezifische Standards
- IT-Sicherheitskatalog

Gesetzliche Forderungen mit Bezug zur Informationssicherheit finden sich unter anderem in folgenden Gesetzen

- IT-Sicherheitsgesetz
- Energiewirtschaftsgesetz
- Patientendaten Schutzgesetz
- Europäische Datenschutzgrundverordnung

Anforderungen an die Informationssicherheit gelten allerdings nicht nur für die freie Wirtschaft, sondern auch im behördlichen Umfeld. Hierbei wurde früher gerne auf den Stand der Technik verwiesen, meist jedoch ohne, dass konkrete Anforderungen benannt wurden. Dies hat sich in den letzten Jahren gewandelt.

IT-Grundschutzprofil

Das Bundesamt für Sicherheit in der Informationstechnik hat im Jahr 2019 das IT-Grundschutz-Profil: Basis-Absicherung Kommunalverwaltung veröffentlicht und im Jahr 2022 aktualisiert. Dieses soll Kommunen eine Grundlage bieten, um die Informationssicherheit durch die Umsetzung von Mindestmaßnahmen sicherzustellen. Ziel ist es, dass die gröbsten Schwachstellen identifiziert und geschlossen werden, um das Schutzniveau anzuheben.

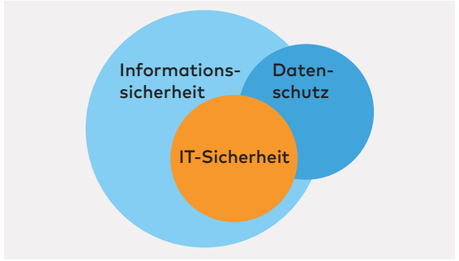


Abbildung: Zusammensetzung der Informationssicherheit

Auszüge aus dem IT-Grundschutz-Profil: „Kommunalverwaltungen sind verpflichtet, ihre IT-Systeme und Verwaltungsvorgänge durch technische und organisatorische Maßnahmen ausreichend abzusichern, auch wenn keine unmittelbare Verpflichtung zur Umsetzung speziell des IT-Grundschutzes aus einer Rechtsnorm abgeleitet werden kann.

Diese Verpflichtungen ergeben sich z. B. aus datenschutzrechtlichen Anforderungen (u. a. EU-Datenschutz-Grundverordnung) und dem Grundsatz des rechtmäßigen Verwaltungshandelns (Rechtsstaatsprinzip Art. 20 Abs. 3 Grundgesetz)."

„IT-Grundschutz-Methodik" [BSI-200-2] und definiert die Mindestsicherheitsmaßnahmen, die in einer Kommunalverwaltung umzusetzen sind, um sich nach hiesiger Einschätzung nicht der groben Fahrlässigkeit schuldig zu machen."

Landtags- und Bundestagswahlen

Doch nicht nur das BSI hat Anforderungen an die Informationssicherheit für Kommunen entwickelt. Für die Landtagswahlen 2021 wurde ein eigenständiger Anforderungskatalog mit 18 Punkten erstellt, welche sich aus 41 Einzelanforderungen aus dem IT-Grundschutz zusammensetzt.

Die Umsetzung der „Maßnahmen für die Ermittlung des vorläufigen Ergebnisses für die Städte, Gemeinden und Landkreise" wurde im Schreiben vom 18.12.2020 empfohlen. Diese Anforderungen galten auch bereits für die Europawahl im Jahr 2018. Ein weiterer Anforderungskatalog wurde den Kommunen für die Bundestagswahl durch das Schreiben der Landeswahlleiter im Juni 2021 übermittelt. Dieser beruht darauf, dass das IT-Grundschutzprofil bereits umgesetzt wurde. Für die Bundestagwahl galten somit 639 Einzelanforderungen, deren Umsetzung im Schreiben der Landeswahlleiter empfohlen wurde. Durch die Aktualisierung des Kommunalprofils hat sich diese Zahl auf 752 Einzelmaßnahmen erhöht.

Deutsche Rentenversicherung

Anforderungen an Kommunen stammen jedoch nicht nur aus dem Umfeld der Wahlen. Die deutsche Rentenversicherung hat für die Teilnahme am Verfahren „eAntrag" eigene Vorgaben definiert., welche aus 123 Einzelanforderungen aus dem IT-Grundschutz bestehen. Anders als bei den Landtags- und Bundestagwahlen muss durch den Behördenleiter eine Verpflichtungserklärung für die Teilnahme am Verfahren „eAntrag" unterschrieben werden. Es gilt somit eine Umsetzungspflicht des Anforderungskatalogs.

Abbildung: Bürotätigkeit in der kommunalen Verwaltung

Kommunalberatung

Der Umgang mit den umfangreichen Anforderungen die das Bundesamt für Sicherheit in der Informationstechnik im Rahmen des IT-Grundschutzprofils für kommunale Verwaltungen fordert, stellt Kommunen und Behörden vor große Herausforderungen. Im Rahmen unserer Kommunalberatung unterteilen wir diese Anforderungen in handhabbare Module, welche wir über einen mehrjährigen Zeitraum Stück für Stück gemeinsam mit einer Kommune umsetzen.

Die Menge an Anforderungen, welche eine Kommune umsetzen soll, scheint im ersten Augenblick viel zu umfangreich, um diese in angemessener Zeit und aufgrund der aktuellen Personalsituation umsetzen zu können. Dies war auch der allgemeine Tenor während und nach den Fortbildungsveranstaltungen („Anwendung des Anforderungskatalogs zur Absicherung des Wahlprozesses „) zur Bundestagwahl im August 2021

Wie bei den meisten, zuerst unüberwindlich scheinenden oder komplexen Aufgaben hilft es, diese in kleinere Pakete zu unterteilen. Dieses Prinzip haben wir auch für die Entwicklung unserer Dienstleistung „Kommunalberatung“ angewendet.

Die geltenden Anforderungen wurden in handhabbare Module unterteilt, welche wir über einen mehrjährigen Zeitraum Stück für Stück gemeinsam mit einer Kommune umsetzen.

Einstieg: Kommunaler QuickCheck?

Für einen ersten Einblick in das bevorstehende Projekt haben wir den kommunalen QuickCheck entwickelt. Dieser kann im Vorfeld beauftragt werden und besteht aus 29 ausgewählten Anforderungen aus dem Gesamtanforderungskatalog, welche das Thema der IT-Sicherheit im Fokus haben. Anhand dieser Stichproben soll Ihnen in einem intensiven Tagesworkshop dargestellt werden, nach welcher

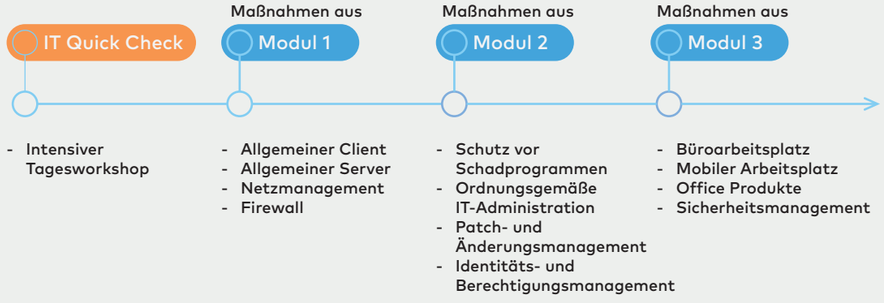


Abbildung: Vorgehensweise zur Umsetzung des Maßnahmenkatalog zum IT-Grundschutz für kommunale Verwaltungen

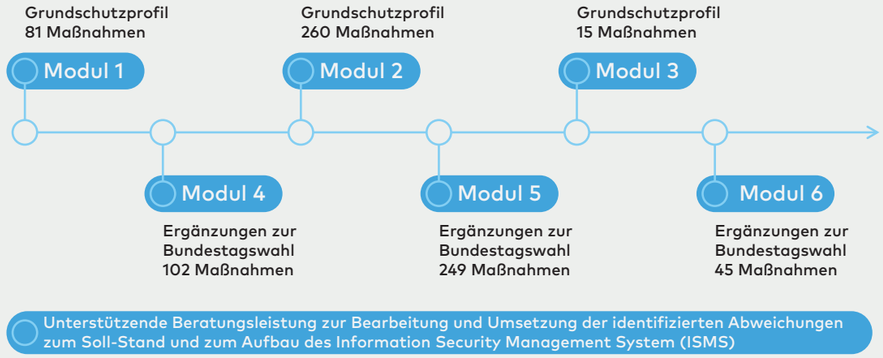


Abbildung: Zeitliche Abfolge unserer Module aus dem Maßnahmenkatalog zum IT-Grundschutz für kommunale Verwaltungen

Methodik wir arbeiten und wie das Gesamtprojekt ablaufen wird. Es handelt sich hierbei jedoch nicht um ein einfaches „Schnupperangebot“. Die Anforderungen sind gezielt so ausgewählt, dass die Durchführung des kommunalen QuickCheck und der Ergebnisbericht einen direkten Mehrwert für ihre Kommune darstellt.

Das Kommunalprofil

Die Grundlage unseres Kommunalprofils bilden die Anforderungen des IT-Grundschutzprofils sowie die ergänzenden Anforderungen für die Bundestagwahl.

Wir haben diese in mehrere Module unterteilt.

Die Module 1-3 beinhalten die Anforderungen des IT-Grundschutzprofils, die Module 4-6 die ergänzenden Anforderungen der Bundestagswahl.

Wir erfassen durch Interviews mit ihren fachlichen Verantwortlichen (oder ihren Dienstleistern) den Ist-Stand der Kommune. Wenn eine Maßnahme nicht erfüllt ist, identifizieren wir Umsetzungsaufgaben, welche bearbeitet werden müssen.

Die konkrete technische oder organisatorische Umsetzung kann hierbei durch Sie, ihre Dienstleister oder unterstützend durch uns erfolgen.

Dafür können Sie auf unser ergänzendes Beratungsmodul zurückgreifen. Einige Aufgaben werden Sie selbst oder ggf. auch Ihr IT-Dienstleister umsetzen müssen, doch bei vielen Themen können wir Sie unterstützen.

Dies umfasst:

- Review bestehender Vorgabedokumente und Überprüfung der Angemessenheit gemäß dem Stand der Technik
- Erstellung notwendiger Richtlinien und Sicherheitskonzept
- Bereitstellung unterstützender Dokumente und Formulare/Protokolle
- Unterstützung bei Prozesseinführungen
- Schulung/Awareness

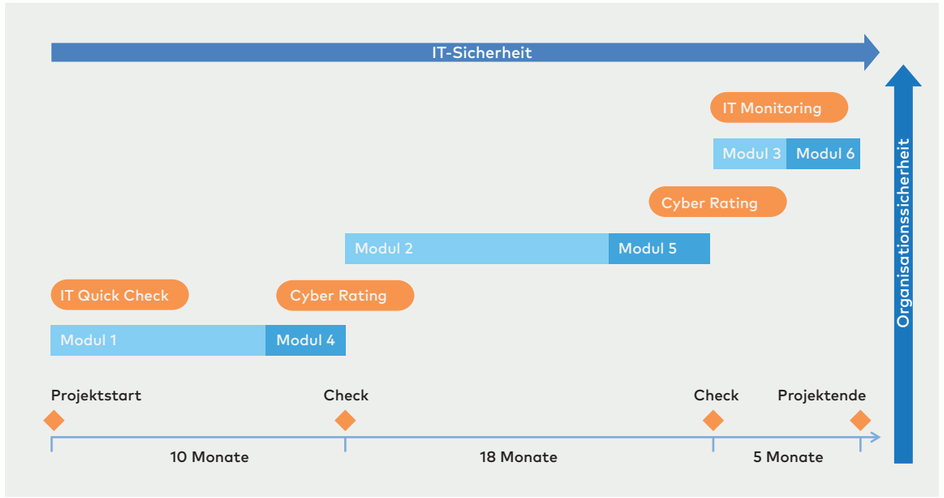
Struktur und Projektablauf

Die Umsetzung beginnt mit Modul 1, welches 81 Einzelanforderungen aus dem IT-Grundschutzprofil umfasst. Dies kann durch Modul 4 (102 Anforderungen der Bundestagswahl) ergänzt werden. Die Einzelanforderungen werden in Termingruppen unterteilt, um diese in ein- bis zweistündigen Terminen mit Ihren Fachverantwortlichen zu bearbeiten.

Die genaue Zeitplanung der einzelnen Termine passen wir an die Verfügbarkeit Ihrer personellen Ressourcen an, um deren Tagesgeschäft nicht übermäßig zu beeinflussen. Dieses Vorgehen wiederholt sich im Projekt für die Bearbeitung der verbliebenen Module.

Der Fokus in den Modulen 1 und 4 liegt auf konzeptionellen Vorgaben wie dem sicheren Informationsaustausch, einem geordneten und sicheren IT-Betrieb sowie ordnungsgemäß verwalteten Fernwartungszugängen und dem Informationssicherheitsverständnis der Mitarbeiter.

Abbildung: Struktur und Projektablauf im zeitlichen Verlauf



In den Modulen 2 und 5 liegt der Fokus auf sicheren IT-Systemen (Clients und Server) sowie der Netzwerkinfrastruktur und den einzelnen Kernanwendungen. Ergänzend dazu wird die physische Infrastruktur und der Zutrittsschutz intensiver beleuchtet. Da es sich hierbei um 260 Einzelanforderungen aus dem Grundschutzprofil sowie 249 für Bundestagswahl handelt, wird die Bearbeitung auch entsprechend mehr Zeit in Anspruch nehmen. Den Abschluss bilden die Module 3 und 6, welche aus insgesamt 60 Einzelanforderungen bestehen, wovon 45 auf die Ergänzungen für die Bundestagswahl fallen.

Zielsetzung und positive Nebeneffekte

Ziel der Umsetzung des Kommunalprofils ist es, den Ist-Stand Ihrer Kommune bzgl. des Erfüllungsgrads der Anforderungen aus dem IT-Grundschutzprofil und den Anforderungen an die Bundestagswahl zu erfassen, Lücken zu identifizieren und diese mit notwendigen Umsetzungsmaßnahmen zu versehen.

Begleitend zum Projekt kann unser Beratungskontingent beauftragt werden, um Sie bei der Umsetzung technischer oder organisatorischer Maßnahmen zu unterstützen.

Die Umsetzung des Kommunalprofils, ergänzt durch die Anforderungen an die Bundestagswahl bietet auch einen direkten und nicht zu vernachlässigenden Vorteil. Durch die Umsetzung der einzelnen Module werden die meisten Anforderungen an die Landtagswahl sowie des eAntrags der Deutschen Rentenversicherung ebenfalls erfüllt. Die dann noch verbliebenen Anforderungen der Landtagswahl und der DRV können mit geringem Aufwand umgesetzt werden.

Eine weitere Zielsetzung von uns ist es, die fachlichen Ansprechpartner während der Projektphase an die Themen der Informationssicherheit, die normative Welt und Struktur der ISO 27001 und des IT-Grundschutzes sowie unserer Arbeitsweise heranzuführen. Sollten Sie uns einen zentralen Ansprechpartner und zukünftigen Verantwortlichen für die Informationssicherheit (= Informationssicherheitsbeauftragter) für die Projektumsetzung benennen, so werden wir diesen fachlich aufbauen, damit dieser zukünftig die Rolle des ISB übernehmen kann.

Denn wie schon durch das BSI im IT-Grundschutzprofil dargelegt, ist die Erfüllung der ausgewählten Einzelanforderungen nur die Grundlage, um die Informationssicherheit in Ihrer Kommune zu gewährleisten. Idealerweise können Ihre Fachverantwortlichen (oder ISB) die Informationssicherheit schrittweise weiter verbessern und mit dem Wandel des Stands der Technik über die Jahre mithalten… auch ohne externer Beratung.

Abbildung: Prozentuale Abdeckung der Anforderungen je Modul

	Modul 7						
	Modul 1	Modul 4	Modul 2	Modul 5	Modul 3	Modul 6	insgesamt
Bundestagswahl	10,7%	13,5%	34,5%	33,1%	1,9%	5,9%	100%
Landtagswahl	11,9%	16,7%	16,7%	30,9%			81,9%
Rentenversicherung	20,2%	14,9%	14,9%	23,4%			81,0%

Ergänzende Dienstleistungen

Kommunale Eigenbetriebe können unter das IT-Sicherheitsgesetz fallen und daher speziellen Anforderungen unterliegen. Überschreiten diese den definierten Schwellwert sind die Anforderungen verpflichtend und deren Umsetzung durch Prüfungen dem Bundesamt für Sicherheit in der Informationstechnik nachzuweisen.

Kommunale Eigenbetriebe

Neben ihrer kommunalen Verwaltung führen Sie eventuell auch Betriebe, welche unter das IT-Sicherheitsgesetz fallen und je nach Versorgungsmenge auch als kritische Infrastruktur gelten.

Am häufigsten trifft dies auf folgende Betriebe zu:

Stadtwerk

Wasser/Abwasser

Abfallentsorgung

Die EnBW Cyber Security GmbH als 100%-Tochter der EnBW AG weiß um die speziellen Anforderungen der verschiedenen Versorgungsbetriebe und die Erfordernisse, welche durch das IT-Sicherheitsgesetz und die Kritis-Verordnung bzw. das Energiewirtschaftsgesetz erfüllt werden müssen. Sowohl bei internen als auch externen Kunden waren wir bereits beratend aktiv und haben diese erfolgreich durch die Prüfungen begleitet.

Wir unterstützen Sie auch hier gerne bei der Erfüllung der Anforderungen. Denken Sie bitte daran: auch wenn ihr Betrieb die Kritis-Schwellwerte nicht überschreitet, gilt die Erfordernis, den Stand der Technik umzusetzen.

Die Umsetzung des Kommunalprofils umfasst diverse IT-technische Anforderungen mit dem Ziel, die IT-Sicherheit in Ihrer Kommune zu verbessern. Hierfür bieten wir ergänzende Dienstleistungen an, die Ihnen neben unserer Beratungsleistung zu speziellen Themen der IT-Sicherheit helfen sollen, diese zu verbessern.

Abbildung: Städtische Wasserversorgung

Cyber Rating

Das Cyber Rating ist eine vollautomatisierte IT-Sicherheitsanalyse und verfolgt das Ziel, eine schnelle und diskrete Ad-Hoc-Bewertung Ihrer IT-Sicherheit zu erhalten. Das Ergebnis des Cyber Ratings stellt eine Außensicht dar, d. h. es werden Informationen, die frei über das Internet verfügbar sind, gesammelt, ohne dabei Ihre internen Prozesse zu beeinträchtigen
.
Prüfkriterien sind, u.a., App-Sicherheit Ihrer aus dem Internet erreichbaren Anwendungen, Abgleich Ihrer Domäne mit über 600 Mio. Blacklist Einträgen, Netzwerksicherheit und Port-Erreichbarkeit Ihrer Systeme, DNS-Konfiguration und Überprüfung auf Fehlkonfigurationen, SSL-Verschlüsselung Protokolle und DSGVO-Konformität. Die Ergebnisse werden in einem ausführlichen Bericht zusammengefasst und in einem ca. 1,5-stündigen Online-Meeting von erfahrenen Analysten, mit präzisen Handlungsempfehlungen für Sie oder Ihre Dienstleister, vorgestellt.

Penetrationstest

Beim Pentest geht es um das manuelle Überprüfen von IT Systemen auf Sicherheitslücken oder auch Schwachstellen. Gefundene Sicherheitslücken werden beim Pentest weitestgehend ausgenutzt, sodass ein realistisches Bild von der Unternehmenssicherheit entsteht. Jede Sicherheitslücke wird dokumentiert, im Anschluss wird das Gefahrenpotenzial eingestuft und Empfehlungen gegeben, wie die Sicherheitslücken gelöst werden können.

Managed IT-Security Monitoring

Unser IT-Security Monitoring besteht aus mehreren Modulen, die sich gegenseitig ergänzen. Vom Schwachstellenmanagement über das IDS Modul bis hin zu hoch automatisierten Netzwerkscans und der Überwachung Ihrer Domain. Auf Ihren Wunsch hin können auch unsere erfahrenen Cyber Security Analysten die aktive Überwachung Ihre Systeme übernehmen.

Abbildung: Managementbericht eines Cyber Ratings

Quellen und Bildnachweise:
Titel: Im Gespräch mit Bürgermeister / EnBW interne Aufnahme, Fotograf: Ines Blersc
Seite 2: Büroarbeit / https://pixabay.com/de/photos/sekretärin-bürojob-büro-office-338561/
Seite 5: Ausdruck IT-Grundschutzprofil / EnBW interne Aufnahme, Fotograf: Uli Deck
Seite 7: Wasserversorgung / EnBW interne Aufnahme , Fotograf: Andy Ridder
Seite 8: CyberRating Dokumente / https://www.pexels.com/de-de/foto/hande-buro-arbeiten-festhalten-7109276/

EnBW Cyber Security GmbH
Ein Unternehmen der EnBW

Durlacher Allee 93
76131 Karlsruhe

Telefon 08000 574847

www.enbw-cybersecurity.com
cybersecurity@enbw.com