Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Einstiegshilfe für die Schwachstellenanalyse von Webportalen

Inhalt

1. *Das BSI im Dienst der Öffentlichkeit*

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft. Als Cybersicherheitsbehörde des Bundes ist es Aufgabe des BSI, Deutschland digital sicher zu machen. Seit seiner Gründung 1991 hat sich das BSI zu einem Kompetenzzentrum für Fragen der Informationssicherheit entwickelt, dessen fachliche Expertise national und international anerkannt ist.

Für die Zukunft Deutschlands ist die Digitalisierung ein wesentlicher Erfolgsfaktor. Voraussetzung einer erfolgreichen Digitalisierung ist die Informationssicherheit. Deshalb beschäftigt sich das BSI damit, in welchen Anwendungsfeldern der Digitalisierung Risiken entstehen können und wie man diese Risiken kalkulierbar und beherrschbar machen kann.

Durch seine ausgeprägte Vernetzung nach innen und außen ist das BSI in der Lage, Know-how in den Bereichen Prävention, Detektion und Reaktion zu bündeln, Themen der Informationssicherheit fachlich zu analysieren und aus der Analyse heraus konkrete Angebote für unterschiedliche Zielgruppen in Staat, Wirtschaft und Gesellschaft abzuleiten. Das BSI nutzt dazu seine integrierte Wertschöpfungskette der Cybersicherheit, die von der Abwehr und Analyse von Cyberangriffen über Beratungsdienstleistungen und Zertifizierungen bis hin zur Entwicklung sicherheitstechnischer Empfehlungen, Best Practices und Standards reicht.

2. *Einleitung*

Im Rahmen der Digitalisierung werden Verwaltungsleistungen elektronisch auf allen föderalen Ebenen und gemeinsam von vielen Verantwortlichen im Rahmen des interoperablen Portalverbunds angeboten.

Der „Umsetzungsplan Bund“ (UP Bund) und das „Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen“ (Onlinezugangsgesetz, OZG) sind im Jahr 2017 in Kraft getreten. Sie bilden die gesetzlichen Grundlagen für die Umsetzung der Cybersicherheitsstrategie des Bundes und die sichere Digitalisierung der gesamten öffentlichen Verwaltung in Deutschland.

Die Bundes-, Landes- und Kommunalverwaltungen stellen aufgrund der Vielzahl an bereitgestellten Webportalen eine große Angriffsfläche und ein besonders attraktives Ziel für Angreifer dar.

Um diese Webportale zu schützen, müssen Schwachstellen frühzeitig gefunden und behoben werden. Hierzu dienen Schwachstellenanalysen durch zertifizierte IT-Sicherheitsdienstleister.

Auf den folgenden Seiten haben wir die wichtigsten Informationen über Schwachstellenanalysen von Webportalen für Verwaltungsleistungen zusammengestellt.

Sie erfahren mehr über

- die Notwendigkeit von Schwachstellenanalysen,
- den Prozessablauf einer typischen Schwachstellenanalyse,
- die besonders beachtenswerten Aspekte innerhalb der einzelnen Schritte sowie
- die weiterführenden Informationsquellen und Ansprechpartnerinnen sowie Ansprechpartner.

Die in dieser Broschüre vorgestellten Abläufe und Informationen sind verkürzt dargestellt, um den Einstieg in die Schwachstellenanalyse zu erleichtern.

3. *Prozessabbildung*

Schritt 1: Festlegung des Betrachtungsgegenstands

Die Entscheidung, was getestet, wie vorgegangen und wie tief getestet wird, wird in dem ersten Schritt festgelegt. Anhand der gewählten Vorgehensweise folgen die nächsten Schritte.

Schritt 4: Untersuchung der Anwendungsebene

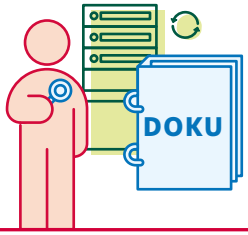
Die Anwendung wird auf Sicherheitsrisiken hin überprüft: Es wird geschaut, ob sich Funktionen der Anwendung ausnutzen lassen und welche Sicherheitsvorkehrungen getroffen wurden.

Schritt 5: Abschlussbericht

Im Abschlussbericht werden die gefundenen Schwachstellen und Sicherheitshinweise aufgeführt, erklärt und in Schadenspotenzial und Ausnutzbarkeit bewertet.

Schritt 2: Auftaktbesprechung

Details werden in einer Besprechung geregelt und festgehalten, genaue Zielsysteme benannt, Testzeiträume festgelegt und (Notfall-)Kontakte geteilt.



Schritt 3: Untersuchung der Prozess-und Systemebene

Untersuchung von Dokumentationen, Abläufen und Konzepten erfolgt. Zusätzlich werden die Absicherungen der Kommunikationsschnittstellen und Betriebssysteme geprüft.

Schritt 6: Abschlussbesprechung

Ein Termin, in dem der Abschlussbericht vorgestellt wird und offene Fragen von allen Beteiligten geklärt werden können.

4. *Motivation und Hintergrund*

Das Onlinezugangsgesetz sieht vor, dass mehr als 6.000 Verwaltungsleistungen auf Kommunal-, Landes- und Bundesebene digital beantragt werden können.

Um dabei die Informationssicherheit zu gewährleisten, hat das Bundesministerium des Innern und für Heimat (BMI) die IT-Sicherheitsverordnung Portalverbund (ITSiV-PV) erstellt. Darin werden weitreichende Anforderungen an die Informationssicherheit aller Komponenten des Portalverbunds sowie an unmittelbar oder mittelbar angebundene Komponenten definiert – also sowohl für Nutzerkonten wie auch für Verwaltungsportale.

Eine Absicherung auf Basis des IT-Grundschutzes ist vorgesehen und Technische Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik müssen beachtet werden. Zusätzlich besteht die Anforderung, dass bei einigen wichtigen Komponenten in regelmäßigen Abständen Schwachstellenanalysen („Penetrationstests“ und „Webchecks“) durchgeführt werden (ITSiV-PV, § 2 Portalverbund und unmittelbar angebundene IT-Komponenten).

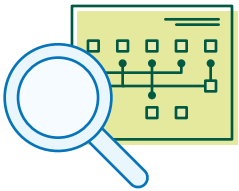
Der UP Bund fordert für die Bundesverwaltung eine Durchführung von Schwachstellenanalysen der Fachanwendungen – mittels Penetrationstests oder Webchecks. Diese sind regelmäßig zu wiederholen und nach größeren Änderungen ebenfalls durchzuführen.

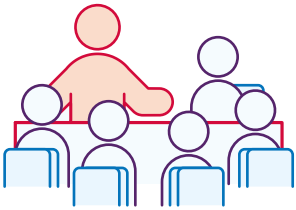
Eine Schwachstellenanalyse für Webportale oder Fachanwendungen sollte möglichst frühzeitig erfolgen. Im besten Fall wird die Anwendung bereits unmittelbar nach Fertigstellung einer Schwachstellenanalyse unterzogen.

Auch wenn Ressourcen für Digitalisierungsprojekte oftmals knapp bemessen sind, reduziert jede vorab gefundene Schwachstelle die Wahrscheinlichkeit eines späteren Schadens durch einen erfolgreichen Cyberangriff erheblich.

Schon gewusst?

Während bei Webchecks – auch bekannt als Web-Application-Penetrationstests – nur ein Blick von außen auf die Webportale vorgenommen wird (genannt „Schlüssellochperspektive“), werden bei einem Penetrationstest (Pentest) neben den öffentlich zugänglichen Systemen auch Hintergrundsysteme und Prozesse untersucht. Penetrationstests sind wesentlich detaillierter und aufwendiger in der Durchführung. Ob ein Webcheck oder ein Pentest sinnvoll ist, muss individuell entschieden werden. Oftmals kann der Betrachtungsgegenstand einen Hinweis liefern, wie im nächsten Kapitel erläutert wird.





5. ***Schritt 1*** – *Festlegung des Betrachtungsgegenstands (Scope)*

Vor der eigentlichen Schwachstellenanalyse sollten zunächst grundsätzliche Fragen geklärt werden.

Dazu wird der Begriff „Scope“ verwendet. Er umfasst den Betrachtungsgegenstand der Untersuchung und seine Rahmenbedingungen, in diesem Fall das Webportal oder die Fachanwendung.

Es gilt zu entscheiden, welche IT-Systeme geprüft werden sollen und in welchem Umfang die Prüfung stattfindet. Das Wissen und Vorgehen werden festgelegt und die Möglichkeit der Angreifer werden simuliert. Insbesondere bei systemübergreifenden Untersuchungen sollten frühzeitig alle involvierten Stellen in Kenntnis gesetzt und in die Planung einbezogen werden.

Es gibt mehrere Entscheidungen zur Sicherheitsanalyse, die im Vorfeld zusammen mit den Beteiligten und dem IT-Sicherheitsdienstleister getroffen werden sollten:

Informationsbasis

Welche Informationen über die Beschaffenheit des Systems erhalten Prüfende? Ist das System dem simulierten Angreifer bekannt, unbekannt oder teilweise bekannt?

Aggressivität

Inwiefern soll es den Prüfenden gestattet sein, das System zu beeinträchtigen, zu übernehmen oder unbrauchbar zu machen?

Umfang

Soll – abhängig von den Ressourcen – eine breite Prüfung oder eine fokussierte, umfangreichere Prüfung einiger weniger Systeme stattfinden?

Vorgehensweise

Wie wichtig ist es, dass der simulierte Angriff durch die Prüfenden von den Prozessbeteiligten unerkannt erfolgt? (Anmerkung: Bei angekündigten Tests auf einer Testumgebung des Webportals sind alle Prozessbeteiligten i. d. R. in Kenntnis gesetzt. Zur Beschleunigung der

Untersuchung sollten bestimmte Schutzmaßnahmen, etwa „Web Application Firewalls“ (WAF), zwischenzeitlich für die Prüfenden deaktiviert werden.

Technik

Über welche weiteren Schnittstellen könnte ein Angreifer versuchen, neben dem offensichtlichen Hauptzugang der Webportale einzudringen? Welche Fernwartungs-, Administrations-, Backup- oder auch Verwaltungsschnittstellen gibt es?

Ausgangspunkt

Soll der simulierte Angriff von außen (Sicht eines „Außentäters“) oder von innen (Sicht eines „Innentäters“) durchgeführt werden? Innentäter haben wahrscheinlich einen Informationsvorsprung, sie können unter Umständen auf weitere Systeme und Berechtigungen zugreifen.

Eine ausführliche Beschreibung der Kriterien und der möglichen Optionen befindet sich im Durchführungskonzept für Penetrationstests:

Eine beispielhafte Auswahl des Scopes wird im Projekt „Markt- und Schwachstellenanalyse zur Sicherheit von E-Government-Apps und Webportalen“ (MaSiGov) beschrieben:

6. ***Schritt 2*** – *Auftaktbesprechung (Kick-off)*

In einem gemeinsamen Termin der Beteiligten, an dem sowohl die Technikverantwortlichen als auch die Prüfenden teilnehmen, wird der Scope der Schwachstellenanalyse finalisiert. Die Details zum genauen Ablauf werden festgelegt und im Rahmen eines „Leistungsscheins" dokumentiert. Idealerweise regelt eine „Vertraulichkeitsvereinbarung" (Non Disclosure Agreement, NDA) zwischen den Parteien den Informationsfluss.

Die nachfolgenden Aspekte sollten vor Beginn der Untersuchung geklärt sein:

Zielsystem

Befindet sich der zu testende Onlinedienst in einer Testumgebung oder einer Produktivumgebung? Da die Produktivumgebung auch regulären Vorgängen dient, sollte hier eine Testumgebung mit einer stabilen Softwareversion, d. h. ohne Änderung während des Testzeitraums, verwendet werden.

Zugänge und Rechte im Rahmen des Tests

Es sollten die von den Prüfenden verwendeten Zugänge, insbesondere IP-Adressen und Konten, klar benannt sein. Zusätzlich sollte feststehen, welche besonderen Rechte diese Zugänge erhalten, etwa eine (zeitlich begrenzte) Umgehung von gewissen Schutzmechanismen zur beschleunigten Prüfung.

Zeitlicher Ablauf des Tests

Es sollte klar sein, welche Komponenten zu welchem Zeitpunkt getestet werden. Dies ist insbesondere dann wichtig, wenn unterschiedliche Komponenten getestet werden oder wenn in einem zweiten Schritt überprüft werden soll, ob die gefundenen Schwachstellen auch bei aktivierten Schutzmechanismen ausnutzbar sind.

Testzeiträume

Der Zeitraum der Tests muss festgelegt werden. Übliche Bürozeiten sollten berücksichtigt werden, da es unter Umständen zu Systemausfällen kommen kann. Ein Plan für das schnelle Wiederverfügbarmachen des Systems muss vorliegen.

Ansprechpersonen

Es sollte klar sein, wer welche Informationen über den Test oder die Ergebnisse erhält. Wie viele Ansprechpersonen und Verantwortliche für die interne Kommunikation gibt es? Wie wird akut auf gefundene kritische Schwachstellen reagiert?

Notfall-Kontakte

Der technische Kontakt bei konkreten, evtl. unvorhergesehenen Ereignissen während der Tests muss klar benannt sein.

Die notwendigen Informationen sollten in Form eines Leistungsscheins festgehalten und allen Beteiligten zur Verfügung gestellt werden. Damit ist klargestellt, welche Aspekte jeweils auf der Prozess-, System- und Anwendungsebene untersucht werden.

7. **Schritt 3** – *Untersuchung der Prozess- und Systemebene*

Unter der „Prozessebene“ werden Abläufe, Konzepte und Dokumentationen verstanden, die einen übergreifenden Charakter haben. Folgende Sachverhalte können untersucht werden:

Dokumentation

Wird der betrachtete Informationsverbund (Scope) vollständig beschrieben und im IT-Sicherheitskonzept berücksichtigt?

Reife betrieblicher Prozesse

Sind Datensicherungs-, Patch- und Änderungskonzepte in funktionierenden Prozessen abgebildet und haben diese den geforderten Reifegrad? Ist das Rollen- und Rechtekonzept wirksam umgesetzt?

Zur „Systemebene“ zählen IT-Systeme wie beispielsweise Server, Desktops oder auch Smartphones. Spezielle, auf dedizierte Funktionen ausgerichtete Computersysteme wie Firewalls oder Router können ebenfalls den IT-Systemen zugeordnet werden. Auf der Systemebene werden die folgenden Sachverhalte untersucht:

Absicherung der Kommunikation

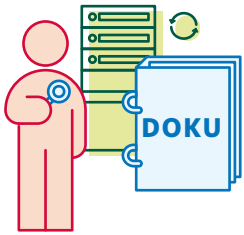
Bei der Untersuchung der Netzwerkschnittstellen werden die offenen Zugänge der Systeme automatisiert ermittelt und festgehalten. Bei den gefundenen Zugängen wird überprüft, welche Dienste angebunden sind und welche Kommunikationsprotokolle verwendet werden.

Absicherung der Betriebssysteme

Auf Betriebssystemebene wird untersucht, ob die laufenden Dienste in einer aktuellen Version vorhanden sind oder ob möglicherweise ältere Versionen mit bekannten Schwachstellen eingesetzt werden.

Abgleich mit den Vorgaben und Empfehlungen des BSI

Das BSI formuliert mit dem „IT-Grundschutz“ und seinen „Technischen Richtlinien“ eine Vielzahl von Anforderungen und gibt Empfehlungen, welche Best Practices darstellen. Beispielsweise kann untersucht werden, inwiefern die eingesetzten kryptografischen Verfahren den Vorgaben und Empfehlungen des BSI entsprechen.



Die nachfolgenden Fragen sollten auf der Systemebene beantwortet werden:

1. Welche Ports sind geöffnet und von außen erreichbar?

2. Welche Dienste sind den erreichbaren Ports in welcher Version zugeordnet?

3. Welche „TLS-Protokollversionen“ werden eingesetzt?

4. Werden die relevanten Technischen Richtlinien des BSI (TR-02102-2 u. TR-03116-4) umgesetzt und ausschließlich die empfohlenen Kombinationen kryptografischer Algorithmen („Cipher Suites“) eingesetzt?

8. ***Schritt 4*** – *Untersuchung der Anwendungsebene*

Die Anwendungsebene umfasst das Webportal oder die Fachanwendung auf der Systemebene. Die Anwendungsebene ist auf die besonders häufig vorkommenden Sicherheitsrisiken hin zu überprüfen.

Zu diesen gehören beispielsweise:

- Fehler in der Zugriffskontrolle
- Fehler in eingesetzten kryptografischen Methoden oder in deren Implementierung
- Unautorisierte Kommandos oder Befehle durch Nutzende
- Unsicheres Architekturdesign der Anwendung
- Sicherheitsrelevante Fehlkonfiguration

Eine Liste der besonders häufig verbreiteten Schwachstellen in Webanwendungen wird regelmäßig vom „Open Web Application Security Project“ (OWASP) herausgegeben.

Bei bereits durchgeführten Schwachstellenanalysen von Webportalen im OZG-Kontext haben sich vor allem folgende Aspekte als anfällig gezeigt:

Authentifizierung & Autorisierung

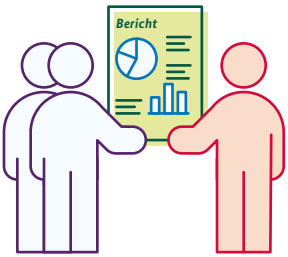
Wie sieht die Anmeldung beim Onlinedienst aus? Eine Open-Redirect-Schwachstelle beispielsweise kann einen Phishing-Angriff begünstigen. Hierbei wird ein Link für den Login am Onlinedienst derart präpariert, dass nach Eingabe der Login-Daten auf der vertrauenswürdigen Seite zu einer gefälschten Website weitergeleitet wird.

Eingabefelder

Wie wird mit den Informationen umgegangen, die eingegeben werden? Findet z. B. eine Rechtschreibprüfung über ein externes Unternehmen statt, so könnte dieses in den Besitz empfindlicher Daten kommen.

Eingesetzte Software oder Drittbibliotheken

Werden neben der Systemebene in der Anwendung externe Ressourcen (z. B. Bibliotheken) eingebunden? Diese Ressourcen werden i. d. R. häufig aktualisiert, um gefundene Schwachstellen zu beseitigen. Daher sollte die Aktualität der verwendeten Bibliotheken sowie der Software regelmäßig überprüft werden.



Dateiupload

Verlangt ein Onlinedienst neben den Antragsdaten weitere Nachweise z. B. von anderen Behörden, die in digitaler Form durch die antragstellende Person hochgeladen werden können? Im Zuge einer Schwachstellenanalyse wird u. a. überprüft, welche Datentypen und Datengrößen akzeptiert werden und ob eine Prüfung auf Schadprogramme stattfindet.

9. ***Schritt 5*** – *Abschlussbericht*

Die Ergebnisse der Schwachstellenanalyse werden in schriftlicher Form festgehalten und den Beteiligten über einen sicheren Kanal, z. B. verschlüsselt über E-Mail oder einen Austauschserver, zur Verfügung gestellt.

Hierbei sollten folgende Aspekte berücksichtigt werden:

Einschätzung der Prüfenden über Schweregrad und Ausnutzbarkeit

Bekannte Schwachstellen haben in der Regel eine Bezeichnung, oftmals eine CVE-Nummer („Common Vulnerabilities and Exposures"), unter der weiterführende Informationen gefunden werden können. Zusätzlich können Schwachstellen entsprechend ihrer Kritikalität bewertet werden, z. B. über den CVSS-Score („Common Vulnerability Scoring System"). Dies erlaubt eine Gewichtung bei der folgenden Beseitigung der Schwachstellen.

Weitere Sicherheitshinweise

Neben den Schwachstellen sollten auch sonstige sicherheitsrelevante Feststellungen Teil des Abschlussberichts sein. Selbst wenn diese nicht unbedingt eigene Schwachstellen darstellen, können sie jedoch begünstigenden Einfluss auf das Schadenspotenzial von Schwachstellen haben.

Zielgruppengerechte Aufteilung und Formulierung

Die Schwachstellen sollten sämtlichen Beteiligten nachvollziehbar erklärt werden. Die IT-Verantwortlichen sollten zudem konkrete Empfehlungen zur Schwachstellenbeseitigung erhalten.

Sofern vereinbart, sollten nach IT-System/Betroffenheit aufgeteilte Abschlussberichte zumindest den Technik-Verantwortlichen weiterführende Informationen liefern: etwa konkrete Prüfprotokolle und Toolauszüge, um die Schwachstellen selbst nachstellen zu können.

10. ***Schritt 6*** – *Abschlussbesprechung*

In der Regel findet eine Abschlussbesprechung nach Fertigstellung des Abschlussberichts statt. Auf folgende Aspekte sollte u. a. geachtet werden:

Gebührender zeitlicher Abstand zur Auswertung des Abschlussberichts

Alle Beteiligten sollten genügend Zeit erhalten, den Abschlussbericht zu lesen. Aufgrund der Aktualität der Prüfung sollte die Abschlussbesprechung jedoch zügig nach dem Erhalt des Abschlussberichts stattfinden.

Gemeinsame Besprechung des Abschlussberichts und der gefundenen Schwachstellen

Der Abschlussbericht sollte gemeinsam mit den jeweils betroffenen Stellen besprochen werden. So wird das gemeinsame Verständnis gefördert. Es empfiehlt sich, dass auch Technik-Verantwortliche anwesend sind.

Klärung von fachlichen und technischen Fragen der Beteiligten

Insbesondere bei gefundenen Schwachstellen und Hinweisen sollten sämtliche offene Fragen, etwa zur Behebung der Schwachstellen oder zu den Empfehlungen der Testenden, ausgeräumt werden.

Klärung des weiteren Vorgehens

Abschließend sollte das weitere Vorgehen geklärt werden. Dies kann intern oder zusammen mit den Testenden erfolgen, etwa in Form eines gezielten Nachtests nach Behebung gefundener Schwachstellen.

11. *Informationsquellen und Ansprechstellen*

Nachdem die Entscheidung für eine Schwachstellenanalyse gefallen ist, ist die Auswahl des IT-Sicherheitsdienstleisters der erste wichtige Schritt. Oftmals gibt es bestehende Rahmenverträge, über die ein Abruf möglich ist.

Der IT-Sicherheitsdienstleister sollte seine Zuverlässigkeit und Unabhängigkeit sowie seine Fachkompetenz und die Qualität der Dienstleistung in Form einer Zertifizierung nachweisen.

Unter nachfolgendem Link ist eine Liste zertifizierter IT-Sicherheitsdienstleister in den Bereichen IS-Revision und IS-Penetrationstests einsehbar:

Häufige Fragestellungen zur richtigen Verhaltensweise bei Sicherheitsvorfällen sowie Informationen über aktuelle Bedrohungen finden Sie hier:

Ansprechpartner für die Bundesverwaltung:

Das BSI bietet die IS-Penetrationstests und IS-Webchecks vorrangig für Bundesbehörden an. Für diese sind die Tests grundsätzlich kostenfrei. Für Anfragen wenden Sie sich bitte an die Kontaktadresse des BSI:
digitalisierungsprojekte@bsi.bund.de

Schon gewusst?

Zwischen Januar 2022 und Januar 2023 wurde das Projekt „Markt- und Schwachstellenanalyse zur Sicherheit von E-Government-Apps und Webportalen“ (MaSiGov) realisiert. Ziel war es, OZG-Portale im Hinblick auf die IT-Sicherheit zu untersuchen und durch die gewonnenen Erkenntnisse die Informationssicherheit der Webportallösungen zu verbessern.
Den Abschlussbericht des Projektes MaSiGov finden Sie unter:

Vorteile in aller Kürze

Die Vorteile einer Schwachstellenanalyse auf einen Blick:

Zusammenfassung

Schwachstellenanalysen verringern die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs und leisten einen Beitrag zur sicheren Digitalisierung der deutschen Verwaltung.

Vorteile

- Strategisches Vorgehen
- Koordiniertes Handeln
- Erfolgreiche und sichere Digitalisierung der Verwaltung
- Risikoreduktion und Abwenden von Imageschäden

Gewinn für Dienstverantwortliche

Mit Schwachstellenanalysen werden sowohl die Informationssicherheit als auch die Einhaltung der gesetzlichen Vorgaben dokumentiert. Eingesetzte personelle und monetäre Ressourcen können in die Verbesserung des Onlinedienstes einfließen. Die Kosten sind wesentlich geringer als bei einem erfolgten Cyberangriff. Die Attraktivität der Lösung für eine Nachnutzung wird erhöht.

Vorteile

- Dokumentation der Informationssicherheit
- Fehler finden und beheben
- Reduktion von Ausfallzeiten
- Langfristiges Einsparen von Ressourcen
- Erhöhung der Reputation
- Kontinuierliche Verbesserung im Informationssicherheitsprozess

Gewinn für technisch Umsetzende

Mit Schwachstellenanalysen können Schwachstellen und Konfigurationsfehler in Onlinediensten gefunden werden. Das Ziel einer Schwachstellenanalyse ist es nicht, Verantwortliche für Schwachstellen ausfindig zu machen. Stattdessen sollen Schwachstellen rechtzeitig vor einem Schadensfall erkannt und behoben werden, um den Onlinedienst abzusichern. Beteiligte können gewonnene Erfahrungen bei zukünftigen Projekten einbringen.

Vorteile

- Umsetzen von Best-Practice-Ansätzen
- Erkennen von Verbesserungspotenzialen
- Wissen vermehren und Fertigkeiten verbessern
- Verantwortung zeigen
- Sicherheitsvorschriften zuverlässig umsetzen

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
Tel.: 0 800 274 1000

Kontakt
bsi@bsi.bund.de

Stand
Februar 2024

Druck
Appel und Klinger Druck & Medien GmbH
Bahnhofstraße 3
96227 Schneckenlohe
www.ak-druck-medien.de

Gestaltung und Illustration
KOMPAKTMEDIEN Agentur für Kommunikation GmbH

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Postfach 20 03 63
53133 Bonn
Tel.: 0800 274 1000
E-Mail: bsi@bsi.bund.de
www.bsi.bund.de