Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: MANAGEMENT

Cyber-Sicherheits-Exposition

Voraussetzung für eine wirksame Absicherung von Netzen und IT-Systemen in Unternehmen, Behörden und anderen Organisationen ist gerade angesichts der hochdynamischen Entwicklung der Bedrohungslage im Cyber-Raum eine möglichst präzise Kenntnis der eigenen Betroffenheit. Einen pragmatischen Ansatz, diese Betroffenheit anhand nachvollziehbarer Maßstäbe zu bestimmen, bildet die *Cyber-Sicherheits-Exposition*.

Ziel

Die hier beschriebene Bestimmung der Cyber-Sicherheits-Exposition soll das Management unterstützen, die eigene reale Betroffenheit herauszuarbeiten, den Schutzbedarf festzustellen und darauf aufbauend das anzustrebende Cyber-Sicherheitsniveau zu definieren.

Anhand der Management-Entscheidung der Cyber-Sicherheits-Exposition ist es dann Aufgabe der Verantwortlichen für IT und IT-Sicherheit (CIO und CISO), daraus Art und Umfang sinnvoller und angemessener Maßnahmen abzuleiten und umzusetzen. Dazu liefern die *Basismaßnahmen der Cyber-Sicherheit* pragmatische Handlungsempfehlungen, deren Beachtung die Grundlagen für robuste Netze und resistente IT-Systeme legt. So werden die Voraussetzungen für eine wirksame Abwehr von Angriffen über das Internet geschaffen.

Mit diesem Vorgehen soll sichergestellt werden, dass angesichts der vielen notwendigen Detailmaßnahmen die wesentlichen Basismaßnahmen der Cyber-Sicherheit stets im Blick behalten werden können.

Bestimmung der Cyber-Sicherheits-Exposition

Die Bestimmung der Cyber-Sicherheits-Exposition der zu schützenden Infrastruktur bildet die Voraussetzung für die Planung und Umsetzung angemessener Maßnahmen und ihre anschließende Bewertung auf Notwendigkeit, Angemessenheit und Wirtschaftlichkeit. Die einzelnen Elemente der Infrastruktur und die dort gespeicherten und übertragenen Daten sowie die Verarbeitungsprozesse selbst sind daher einer ganzheitlichen Cyber-Bedrohungsanalyse zu unterziehen. Zur Orientierung über gängige Cyber-Angriffe kann das *Register aktueller Cyber-Gefährdungen und -Angriffsformen* des BSI[1] genutzt werden.

Die zu schützende IT-Infrastruktur sowie deren einzelne Elemente sind einem breiten Spektrum von Angriffsmethoden ausgesetzt. Die daraus folgende Cyber-Sicherheits-Exposition der gespeicherten und übertragenen Daten und Prozesse lässt sich aus der Betrachtung des Zusammenwirkens unterschiedlicher Faktoren systematisch erfassen.

Die Cyber-Sicherheits-Exposition kann die Werte **normal**, **hoch** oder **sehr hoch** annehmen und orientiert sich damit an der Schutzbedarfsfeststellung nach dem BSI-Standard 100-2 *IT-Grund-*

1 https://www.bsi.bund.de/ContentBSI/Themen/Cyber-Sicherheit/Analysen/Grundlagen/BSIa001.html

schutz-Vorgehensweise. Diese Werte werden durch mehrere Faktoren bestimmt: die *Attraktivität* der zu schützenden Infrastruktur, die *Charakterisierung der Angreifer*, der *Wert* der angegriffenen Daten und Prozesse, die *Zielgerichtetheit* der Angriffe und ob bereits Erfahrungswerte zu *Angriffen in der Vergangenheit* vorhanden sind. Dabei existiert die Cyber-Sicherheits-Exposition sowohl in Bezug auf die *Vertraulichkeit* als auch die *Verfügbarkeit* sowie die *Integrität*. Die Cyber-Sicherheits-Exposition ist schließlich im Hinblick auf die *Transparenz* der Infrastruktur für Angreifer zu gewichten.

Damit ergeben sich folgende **Leitfragen** zur Bestimmung der Cyber-Sicherheits-Exposition:

- *Wert der Informationen und Prozesse*
  - Welche **Daten** stellen den größten Wert dar, sowohl im Hinblick auf ihre *Vertraulichkeit* als auch ihre *Verfügbarkeit* und *Integrität*?
  - Welche **Prozesse** stellen den größten Wert dar, sowohl im Hinblick auf ihre *Vertraulichkeit* als auch ihre *Verfügbarkeit* und *Integrität*?
  - Wie abhängig sind geschäftskritische Prozesse der Institution von den Daten?
- *Attraktivität für Angreifer*
  - Wie attraktiv ist es für Angreifer, Zugriff auf die vertraulichen Daten zu erlangen?
  - Wie attraktiv ist es für Angreifer, die Verfügbarkeit der Daten oder Prozesse einzuschränken?
  - Wie attraktiv ist es für Angreifer, die Integrität der Daten oder Prozesse durch Manipulationen zu verletzen?
- *Charakterisierung der Angreifer*
  - Wer kommt für Angriffe gegen die Vertraulichkeit, die Verfügbarkeit und/oder die Integrität in Betracht?
    - Täter, die in ihrer Freizeit und aus reiner Neugier agieren (Hobbyisten)?
    - IT-Sicherheitsforscher, die zunächst ein akademisches Interesse in Bezug auf Angriffsmöglichkeiten verfolgen, ihre Ergebnisse dann jedoch auch breit veröffentlichen (Full Disclosure)?
    - Cyber-Kleinkriminelle, für die insbesondere die monetäre Verwertbarkeit erbeuteter Daten im Vordergrund steht?
    - Professionelle, organisierte Cyber-Kriminelle, auch professionelle Konkurrenz-Spionage?
    - Hacktivisten, die mit ihren Angriffen politische und gesellschaftliche Ziele verfolgen?
    - Staatliche Stellen wie z. B. Nachrichtendienste, die auf umfangreiche Ressourcen zur Planung und Durchführung ihrer Angriffe zurückgreifen können?
- *Zielgerichtetheit der Cyber-Angriffe*
  - Ist davon auszugehen, dass die Institution von **Flächenangriffen** betroffen sein wird, deren Ziele diese Angreifergruppen eher zufällig in großer Zahl auswählen?
  - Oder ist zu vermuten, dass die Institution **gezielt angegriffen** wird, was eine bessere Vorbereitung und Durchführung des Angriffs erlaubt?
- *Erfahrungswerte über Angriffe in der Vergangenheit*
  - Sind in der Vergangenheit Cyber-Angriffe auf die Institution detektiert worden?
  - Gab es in der Vergangenheit erfolgreiche Cyber-Angriffe, die zu Schäden geführt haben?

Aus dieser Analyse lässt sich dann die Cyber-Sicherheits-Exposition in Bezug auf die Schutzziele *Vertraulichkeit*, *Verfügbarkeit* und *Integrität* orientiert an den in den Tabellen 1, 2 und 3 definierten Berechnungsgrundlagen bestimmen. Dabei ist zunächst in jeder Zeile dem Bedrohungssgrad der *Vertraulichkeit*, *Verfügbarkeit* und *Integrität* in Bezug auf die angegebenen Kriterien ein individueller Punktwert zuzuordnen, aus dem dann der maximale Wert für jeden Grundwert ermittelt wird.

Bestimmung des Bedrohungsgrads	***Vertraulichkeit***	***Verfügbarkeit***	***Integrität***
Wert der Daten und Prozesse	gering **0** normal **1** hoch **2** sehr hoch **4**	gering **0** normal **1** hoch **2** sehr hoch **4**	gering **0** normal **1** hoch **2** sehr hoch **4**
Attraktivität für Angreifer	gering **0** normal **1** hoch **2** sehr hoch **4**	gering **0** normal **1** hoch **2** sehr hoch **4**	gering **0** normal **1** hoch **2** sehr hoch **4**
Art der Angreifer	Hobbyisten **0** Forscher **1** Kleinkriminelle **2** prof. Kriminelle **4** Hacktivisten **4** staatl. Akteure **5**	Hobbyisten **0** Forscher **1** Kleinkriminelle **2** prof. Kriminelle **4** Hacktivisten **4** staatl. Akteure **5**	Hobbyisten **0** Forscher **1** Kleinkriminelle **2** prof. Kriminelle **4** Hacktivisten **4** staatl. Akteure **5**
Zielgerichtetheit des Angriffs	Flächenangriff **1** gezielter Angriff **5**	Flächenangriff **1** gezielter Angriff **4**	Flächenangriff **1** gezielter Angriff **5**
Angriffe in der Vergangenheit	unbekannt **1** abgewehrt **3** erfolgreich **5**	unbekannt **1** abgewehrt **3** erfolgreich **5**	unbekannt **1** abgewehrt **3** erfolgreich **5**
	Maximum ↓	Maximum ↓	Maximum ↓
Bedrohungsgrad	max. Punktwert **1 … 5**	max. Punktwert **1 … 5**	max. Punktwert **1 … 5**

Tabelle 1: Bestimmung des Bedrohungsgrades

Für die erfolgreiche Durchführung eines Cyber-Angriffes benötigt der Angreifer möglichst viele Informationen über die angegriffene Institution. Hierbei ist ausschlaggebend, wie **transparent** sich die Institution für den Angreifer darstellt:

- *Welche Informationen über den Aufbau der zu schützenden Infrastruktur sind öffentlich verfügbar?*
  - Können aus dem Internetauftritt der Behörde oder des Unternehmens Rückschlüsse auf die IT-Infrastruktur gezogen werden?
  - Welche Informationen werden über Stellenangebote für technisches Personal preisgegeben?
  - Enthalten Veröffentlichungen der Behörde oder des Unternehmens, wie Geschäftsberichte oder (insbesondere in der öffentlichen Verwaltung) durchgeführte Beschaffungen, direkte oder indirekte Angaben über die IT-Infrastruktur?
  - Wie verhalten sich Angehörige der Behörde oder des Unternehmens beruflich und privat in Sozialen Netzen? Welche Informationen zur technischen Ausstattung geben sie dabei bewusst oder unbewusst preis? Welche Rückschlüsse auf Schlüsselpositionen in der Organisation und mögliche technische und menschliche Einfallstore sind möglich?

- *Können Angreifer mit technischen Methoden Einzelheiten der Infrastruktur aufklären?*
  - Welche technischen Daten werden von den mit dem Internet verbundenen Systemen nach außen weitergegeben, z. B. von Webservern einer Organisation?
  - Können durch die Analyse der von Internet-Browsern der Organisation beim Aufruf von externen Webseiten mitgesendeten Informationen Details der installierten Software in Erfahrung gebracht werden?
  - Enthalten die Datenfelder von E-Mails der Behörde oder des Unternehmens z. B. Informationen über die eingesetzte Groupware und deren Struktur?
  - Sind in Dokumenten der Behörde oder des Unternehmens offene oder versteckte Metadaten enthalten, die unbeabsichtigt weitere Informationen preisgeben?
- *Werden über die Behörde oder das Unternehmen von Dritten in halboffenen oder geschlossenen Foren im Internet Informationen gesammelt, die für Angreifer, die diese Foren beobachten, von Nutzen sein könnten?*

Für die nachfolgende Festlegung der Cyber-Sicherheits-Exposition sind nun die Werte für den Aspekt **der Transparenz** zu klassifizieren.

Bestimmung der Transparenz	***Vertraulichkeit***	***Verfügbarkeit***	***Integrität***
Transparenz für den Angreifer		**gering –1** **mittel 0** **hoch +1**	

Tabelle 2: Bestimmung der Transparenz

Die Cyber-Sicherheits-Exposition bestimmt sich jetzt aus der **Summe** des Bedrohungsgrads und des Transparenzwerts

Cyber-Sicherheits-Exposition = Bedrohungsgrad + Transparenz

und kann Werte zwischen 0 und 6 annehmen, die zu einer **normalen**, **hohen** oder **sehr hohen** Cyber-Sicherheits-Exposition führen.

Bestimmung der Cyber-Sicherheits-Exposition		***Vertraulichkeit***	***Verfügbarkeit***	***Integrität***
Cyber-Sicherheits-Exposition	**normal**	max. Punktwert **0 … 1**	max. Punktwert **0 … 1**	max. Punktwert **0 … 1**
	hoch	max. Punktwert **2 … 3**	max. Punktwert **2 … 3**	max. Punktwert **2 … 3**
	sehr hoch	max. Punktwert **4 … 6**	max. Punktwert **4 … 6**	max. Punktwert **4 … 6**

Tabelle 3: Bestimmung der Cyber-Sicherheits-Exposition

Die Darstellung der Cyber-Sicherheits-Exposition erfolgt dabei immer getrennt für Vertraulichkeit, Verfügbarkeit und Integrität:

Cyber-Sicherheits-Exposition = (***Vertraulichkeit*** | ***Verfügbarkeit*** | ***Integrität***)

Beispiel für ein fiktives Industrieunternehmen:

- Als Angreifer gegen die Vertraulichkeit von Unternehmensdaten im Rahmen einer Industriespionage sind staatliche Akteure in Betracht zu ziehen.
- Es ist jedoch nicht damit zu rechnen, dass es Angreifer gibt, für die bei diesem Unternehmen eine Beeinträchtigung der Verfügbarkeit ein interessantes Ziel darstellt (etwa in Form von Distributed-Denial-of-Service-Angriffen). Eine kurzfristige Nichtverfügbarkeit von Diensten stellt auch kein besonderes Risiko für das Unternehmen dar.
- Gleichwohl wäre die Schadenshöhe bei Angriffen gegen die Integrität der Daten, orientiert an deren Wert für das Unternehmen, als hoch abzuschätzen.
- Die Transparenz des Unternehmens aus Sicht des Angreifers liegt im mittleren Bereich.
- In diesem Fall ergibt sich ein maximaler Punktwert für die Vertraulichkeit von 5, für die Verfügbarkeit von 1 und die Integrität von 2. Dies führt zu folgender formalen Exposition:

  Cyber-Sicherheits-Exposition = (*Vertraulichkeit* **sehr hoch** | *Verfügbarkeit* **normal** | *Integrität* **hoch**)

- Die so bestimmte Cyber-Sicherheits-Exposition fasst die Bedrohungslage für die untersuchte Infrastruktur in Bezug auf die Transparenz und Attraktivität für Angreifer, die Art und Zielgerichtetheit der Angreifer, mögliche Schadenshöhen sowie Erkenntnisse zu bereits stattgefundenen Angriffen zusammen und bildet damit das entscheidende Kriterium dafür, welche Maßnahmen in den Schlüsselbereichen der Cyber-Sicherheit in welcher Intensität zu ergreifen sind.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an cs-info@bsi.bund.de gesendet werden.