Bundesamt für Verfassungsschutz

initiative wirtschaftsschutz

Gemeinsam. Werte. Schützen.

Abteilung Cyber- und Spionageabwehr

Datensparsamkeit zur Minimierung von Gefahren für KRITIS

Datensparsamkeit zur Minimierung von Gefahren für KRITIS

Inhalt

1. Einführung

Das Thema Datensparsamkeit gewinnt in der digital vernetzten Welt, insbesondere im Bereich der Kritischen Infrastrukturen (KRITIS), wie Stromnetze, Wasserversorgungssysteme oder Verkehrsleitsysteme, zunehmend an Bedeutung. Diese Infrastrukturen sind essenziell für die Aufrechterhaltung der öffentlichen Sicherheit, der Wirtschaft und der Versorgungslage der Bevölkerung. Sie basieren auf komplexen Informationstechnologien und vernetzten Systemen, die sie anfällig für Cyberangriffe machen. Derartige Angriffe können zu weitreichenden Störungen führen, die nicht nur die betroffenen Einrichtungen beeinträchtigen, sondern auch gravierende Folgen für die Gesellschaft haben können.

2. Problemstellung

Die Verfügbarkeit von Informationen über KRITIS im Internet und anderen öffentlichen Plattformen stellt ein signifikantes Sicherheitsrisiko dar. Informationen, die auf den ersten Blick harmlos erscheinen mögen, wie Netzpläne oder Details zu technischen Systemen, können von potenziellen Angreifern missbraucht werden, um Sicherheitslücken zu identifizieren und auszunutzen. Es besteht daher die Notwendigkeit, eine sorgfältige Abwägung hinsichtlich Art, Umfang und Zugänglichkeit von veröffentlichten Informationen vorzunehmen.

Insbesondere gesetzlich vorgegebene Informationspflichten nehmen eine bedeutende Rolle in der Förderung der öffentlichen Zugänglichkeit und des Verständnisses kritischer Infrastrukturen ein, bergen jedoch gleichzeitig das Risiko, den Grundsatz der Datensparsamkeit zu untergraben. Die Gefahr besteht, dass potenziell sensible oder sicherheitskritische Informationen von unautorisierten Personen oder Gruppen für schädliche Zwecke missbraucht werden könnten. In der Publikation von UP KRITIS[1]

[1] Die UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betreibt die Geschäftsstelle des UP KRITIS.

bezüglich der Sicherheitsaspekte und gesetzlichen Informationspflichten für Betreiber kritischer Infrastrukturen werden vertiefende Einblicke in die Thematik bereitgestellt.[2]

In seinen Warn- und Sicherheitsmitteilungen unterstreicht auch das Bundesamt für Verfassungsschutz (BfV) die akuten Risiken, denen Betreiber Kritischer Infrastrukturen gegenüberstehen.[3] Besonders hervorgehoben werden die Gefahren, die durch leicht zugängliche, detaillierte Darstellungen in Präsentationen und auf Karten, durch öffentlich einsehbare interne Ablaufpläne und Kontaktdaten, sowie durch anfällige Systeme infolge von Port-, Service- und Schwachstellen-Scans entstehen. Zusätzlich werden Informationen in Stellenausschreibungen als potenzielle Sicherheitslücken beschrieben. Als Gegenmaßnahmen empfiehlt das BfV die regelmäßige Sensibilisierung und Weiterbildung von Angestellten, eine kritische Überprüfung sämtlicher Veröffentlichungen, die Etablierung sicherer Kommunikationswege, die Durchführung von Penetrationstests sowie eine strikte Kontrolle des Zugriffs auf interne Serverdienste über das Internet. Vertiefende Einblicke in die Thematik finden sich auch in den vom BfV herausgegebenen Publikationen zum Wirtschaftsschutz.[4]

3. Handlungsempfehlungen zur Reduzierung des Gefahrenpotenzials

3.1 Grundprinzip der Datensparsamkeit

Die Veröffentlichung von Informationen sollte immer unter dem Prinzip der Datensparsamkeit erfolgen. Dies bedeutet, dass nur solche Informationen freigegeben werden, die für den vorgesehenen Zweck unbedingt erforderlich sind. Informationen, die potenziell sicherheitskritisch sein könnten, sollten zurückgehalten oder nur in generalisierter Form veröffentlicht werden.

[2] Vgl. „Sicherheitsaspekte und Hinweise für die Betreiber Kritischer Infrastrukturen im Kontext zu gesetzlichen Transparenzpflichten“ vom 02.05.2022, abrufbar unter: www .bsi.bund.de/dok/1043080; zuletzt abgerufen am 04.09.2024.

[3] Die Veröffentlichungen des BfV sind abrufbar unter www .verfassungsschutz.de.

[4] Insbesondere sind die BfV Publikationsreihen „Sicherheitshinweis für die Wirtschaft“, „Informationsblätter zum Wirtschaftsschutz“, das „SPOC-Magazin“ und der BfV „Cyber-Brief“ für Betreiber von KRITIS relevant.

3.2 Risikobewertung und Risikomanagement

Im Rahmen des Risikomanagements ist die kontinuierliche Risikobewertung ein zentraler Aspekt, der eine dynamische und angepasste Reaktion auf eine sich ständig ändernde Bedrohungslandschaft ermöglicht. Ein wesentliches Element dabei ist die Identifikation von Informationen, deren Veröffentlichung ein Sicherheitsrisiko darstellen könnte. In diesem Kontext spielt die Kenntnis über Methoden und Werkzeuge, die Angreifer nutzen könnten, eine wichtige Rolle.

Beispielsweise könnten frei nutzbare Techniken wie etwa der Einsatz von „Google Dorks“ – die geschickte Kombination von Suchoperatoren oder Schlüsselwörtern oder die Nutzung der Google Hacking Database von potenziellen Angreifern eingesetzt werden, um auf sensible Informationen zuzugreifen, die unbeabsichtigt oder durch mangelnde Datensparsamkeit im Internet veröffentlicht wurden. Diese Suchtechniken ermöglichen es, spezifische Abfragen zu formulieren, die auf die Entdeckung von exponierten sensiblen Daten abzielen, wie etwa offene Datenbanken, nicht gesicherte Verzeichnisse oder spezifische Dateitypen, die vertrauliche Informationen enthalten könnten.

Die Bewertung der potenziellen Folgen eines Informationslecks umfasst nicht nur die direkten Auswirkungen auf die Datensicherheit und die Integrität der betroffenen Systeme, sondern auch die weiterreichenden Konsequenzen für das Ansehen der Organisation, rechtliche Haftung und mögliche finanzielle Verluste. Diese umfassende Sichtweise ist entscheidend, um Prioritäten bei der Implementierung von Schutzmaßnahmen zu setzen und Ressourcen effektiv zu allokieren.

Um der Bedrohung durch solche Angriffstechniken entgegenzuwirken, ist es notwendig, Sicherheitsmaßnahmen zu ergreifen, die sowohl präventiver als auch reaktiver Natur sind. Dazu gehören die Implementierung von Sicherheitsrichtlinien, die die Veröffentlichung von Informationen regeln, die Verschlüsselung von sensiblen Daten sowie die Sicherung von Webanwendungen und Datenbanken gegen unbefugten Zugriff.

3.3 Sicherheitsrichtlinien und Sicherheitsstandards

Die Entwicklung und Implementierung von Sicherheitsrichtlinien und -standards ist entscheidend, um den Schutz von KRITIS zu gewährleisten. Dazu gehört auch die

Festlegung von Richtlinien für die Veröffentlichung von Informationen, die Sicherstellung der Datenintegrität und die Regulierung des Zugangs zu sensiblen Daten.

3.4 Sensibilisierung und Schulung

Die Sensibilisierung und Schulung von Mitarbeitenden und der Öffentlichkeit spielen eine wichtige Rolle bei der Prävention von Sicherheitsvorfällen. Ein besseres Verständnis für die Bedeutung von Datensparsamkeit und die Risiken, die mit der Veröffentlichung von sicherheitsrelevanten Informationen verbunden sind, kann dazu beitragen, das Gefahrenpotenzial zu reduzieren.

3.5 Technische und organisatorische Maßnahmen

Technische Sicherheitsmaßnahmen, wie Verschlüsselung, Zugriffskontrollen und regelmäßige Sicherheitsüberprüfungen, sind ebenso wichtig wie organisatorische Maßnahmen, einschließlich der Entwicklung von Notfallplänen und der Etablierung klarer Verantwortlichkeiten im Bereich der Informationssicherheit.

3.6 Threat Intelligence

Die Integration von Threat Intelligence in das Risikomanagement und in Strategien zur Reduzierung des Gefahrenpotenzials spielt eine entscheidende Rolle. Durch die Nutzung von Threat Intelligence können Unternehmen potenzielle Angriffsvektoren und die Taktiken, Techniken sowie Verfahren (TTPs) von Cyberakteuren proaktiv identifizieren. Diese Informationen ermöglichen es, Schwachstellen zu erkennen, bevor sie von Angreifern ausgenutzt werden können, und bilden eine solide Grundlage für die Entwicklung präventiver Maßnahmen. Threat Intelligence sollte in bestehende Sicherheitstools und -prozesse integriert werden, um automatisierte Entscheidungsfindungen zu unterstützen. Beispielsweise kann die Integration in Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM)-Systeme oder Endpunktschutzlösungen die Erkennung und Abwehr von Angriffen verbessern.

4. Fazit

Die Balance zwischen der Notwendigkeit, Informationen öffentlich zugänglich zu machen, und dem Schutz Kritischer Infrastrukturen vor Cyberangriffen und Sabotage ist eine kontinuierliche Herausforderung. Datensparsamkeit spielt eine entscheidende Rolle im Schutz, da sie das Gefährdungspotenzial durch öffentlich zugängliche Informationen minimiert. Unternehmen und Organisationen müssen sich der Risiken bewusst sein und proaktiv Maßnahmen ergreifen, um sensible Informationen bestmöglich zu schützen, während sie gleichzeitig die gesetzlichen und gesellschaftlichen Anforderungen an Transparenz und Informationsfreigabe erfüllen.

5. Ausblick und Weiterentwicklung

In einer sich schnell verändernden digitalen Landschaft müssen die Praktiken der Datensparsamkeit und Sicherheitsmaßnahmen regelmäßig überdacht und angepasst werden. Die Einführung neuer Technologien und die Evolution von Cyberbedrohungen erfordern eine agile Sicherheitskultur, die in der Lage ist, auf neue Herausforderungen effektiv zu reagieren. Der Schutz kritischer Infrastrukturen ist eine gemeinschaftliche Aufgabe, die eine enge Zusammenarbeit zwischen dem privaten Sektor, den Sicherheitsbehörden und der Zivilgesellschaft erfordert.

Die Implementierung von Datenschutzprinzipien, die Entwicklung von Resilienz gegenüber Cyberangriffen und die Förderung einer Sicherheitskultur sind Schlüsselelemente, um das Fundament Kritischer Infrastrukturen zu stärken. Indem die Veröffentlichung von potenziell riskanten Informationen minimiert wird und gleichzeitig die Sicherheit der Systeme maximiert wird, kann Versorgungssicherheit, wirtschaftliche Stabilität und öffentliche Sicherheit in einer zunehmend vernetzten Welt gewährleistet werden.

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Abteilung Cyber- und Spionageabwehr
Merianstraße 100
50765 Köln
poststelle@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0) 228/99 792-0
Fax: +49 (0) 228/99 10 792-2915

Bildnachweis
© Avege – stock.adobe.com

Stand
September 2024