Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

Oktober 2024

Empfehlungen für die Sicherheitsüberprüfung von Personen in Unternehmen

1 Einführung

Integrität und Vertrauenswürdigkeit der Mitarbeitenden sind in der heutigen Geschäftswelt von entscheidender Bedeutung. Durch gründliche Überprüfungen können Unternehmen potenzielle Risiken minimieren und sicherstellen, dass sie nur vertrauenswürdigen Personen Zugang zu sensiblen Daten, finanziellen Ressourcen oder kritischen Systemen gewähren.

Das Ziel solcher Überprüfungen ist sicherzustellen, dass die überprüfte Person kein Sicherheitsrisiko darstellt. Es dürfen keine Zweifel an ihrer Integrität, Zuverlässigkeit und Vertrauenswürdigkeit bestehen. Zudem soll die Person aufgrund ihrer Lebensumstände weder erpressbar noch bestechlich sein.

Die Anforderung zur Durchführung einer solchen Prüfung, sowie die Konsequenzen, falls ein negatives Resultat ermittelt wird, sollten sowohl im Einstellungsprozess als auch im Arbeitsvertrag fest verankert sein. Dabei muss auch die Einhaltung des Bundesgesetzes über den Datenschutz[1] berücksichtigt werden.

Diese Empfehlung zeigt auf, was sinnvollerweise zur Überprüfung berücksichtigt werden sollte und wie die verschiedenen Aspekte bewertet werden können. Sie unterstützt insbesondere Unternehmen, die aufgrund von Compliance Anforderungen solche Überprüfungen durchführen müssen, dazu gehören unter anderem Unternehmen in den Bereichen Strom- und Gas, die den IKT-Minimalstandard berücksichtigen müssen.[2]

[1] Datenschutzgesetz; DSG; SR 235.1.

[2] Der Bundesrat hat in der Stromversorgungsverordnung (StromVV; SR 734.71) Unternehmen der Profile A und B in den Sektoren Strom und Gas zur Einhaltung gewisser Anforderungen des IKT-Minimalstandard des Bundesamtes für wirtschaftliche Landesversorgung (BWL) verpflichtet. Dies beinhaltet unter anderem auch die Aufgabe, dass für bestimmte Rollen eine Sicherheitsüberprüfung durchgeführt werden muss (Siehe auch IKT-Minimalstandard BWL, Version 1.1 Aktivität: PR.IP-11 oder nach NIST Cyber Security Framework 2.0, die Funktion GV.PR-04).

2 Prüfpunkte und Bewertung

Die Sicherheitsüberprüfung umfasst Massnahmen wie die Prüfung der Identität und Einsicht in verschiedene Register. Sie kann auch das persönliche Umfeld der betroffenen Person miteinbeziehen, um ein umfassendes Bild ihrer Vertrauenswürdigkeit zu erhalten. Folgende Massnahmen ermöglichen eine aussagekräftige Einschätzung.

Prüfpunkt	Prüfziel, Beurteilungsdimension
Strafregisterauszug	Der eingeforderte Strafregisterauszug zeigt keine Einträge, welche die Vertrauenswürdigkeit beeinträchtigen. Sofern problematischen Einträge vorhanden sind, kann die zu prüfende Person angefragt werden, allfällige Urteile bzw. Strafbefehle (freiwillig) offenzulegen, damit die Einträge besser beurteilt werden können.
Betreibungsregister-auszug	Der Betreibungsregisterauszug zeigt keine Einträge, welche auf eine Bestechlichkeit hinweisen. Eine Selbstdeklaration von Privatkrediten zur Tilgung von Schulden kann bei der Beurteilung der Einträge unterstützend wirken. Die zu prüfende Person sollte informiert werden, dass sie bei allfälligen missbräuchlichen Einträgen die Details dazu (freiwillig) offenlegen kann.
Soziale Medien und Internet	Die Recherche in öffentlichen Quellen, z.B. Internet und Sozialen Medien, erlaubt es zu erkennen, ob Teilnahmen an unpassenden Veranstaltungen stattgefunden haben oder ob etwaige Posts die Integrität oder Loyalität in Frage stellen, respektive die Person bestechlich machen.
Diplome und Zertifikate	Die Verifikation von vorgelegten Diplomen beim jeweiligen Aussteller erlaubt es, die Korrektheit zu bestätigen. Fälschungen beeinträchtigen die Integrität und Vertrauenswürdigkeit der Person.
Auslandverbindungen	Auslandsverbindungen durch Herkunft oder längeren Aufenthalt können auf eine problematische Einflussnahme eines fremden Staates oder auf Erpressbarkeit hindeuten (z.B. Bedrohung der dort lebenden Familie) und erfordern eine Prüfung der Vertrauenswürdigkeit. Falls eine Überprüfung ausländischer Personen aufgrund fehlender internationaler Abkommen oder zeitlicher Beschränkungen nicht möglich ist, kann das Unternehmen das Risiko übernehmen und dies im Risikomanagement-prozess dokumentieren.
Arbeitszeugnisse und Arbeitgebende	Falsche Angaben zu früheren Arbeitgebenden oder Kündigungsgründe können die Integrität und Vertrauenswürdigkeit in Frage stellen. Deshalb können hier Rückfragen zu Arbeitszeugnissen, die Verifikation von Anstellungen, und allenfalls Kündigungsgründe von ehemaligen Arbeitgebenden unterstützen.
Interviews	Interviews erlauben es, die Punkte nochmals zu verifizieren.

3 Sicherheitsüberprüfung als Teil der Organisatorischen Prozesse

- **Bewerbung**: Bei der Bewerbung muss die Einwilligungserklärung zur Durchführung der Sicherheitsüberprüfung ein Teil des Verfahrens sein. Die Kandidatin oder der Kandidat muss darüber informiert werden.
- **Nachträgliche Sicherheitsüberprüfungen**: Wenn Mitarbeitende nach der Anstellung aufgrund von neuen Verpflichtungen eine Sicherheitsüberprüfung durchlaufen müssen, muss der Vertrag gegebenenfalls angepasst werden.
- **Nachprüfungen**: Prüfungen sollten regelmässig wiederholt werden, je nach Kritikalität sollte dies alle zwei bis fünf Jahre, sowie bei einem Funktionswechsel gemacht werden. Wir empfehlen, dass Arbeitgebende die Auszüge für die Nachprüfung direkt beziehen, um den Prozess zu vereinfachen.
- **Prüfkriterien**: Das Unternehmen muss die Kritikalität von Einträgen im Straf- oder Betreibungsregister definieren und einen Prozess zur Beurteilungs- und Entscheidungsfindung ausarbeiten. Entscheide und Interviews sollten, wenn möglich im 4-Augen Prinzip stattfinden, um die Qualität der Bewertung zu erhöhen.
- **Ablage der Resultate und Datenschutz**: Die Resultate der Prüfung müssen datenschutzkonform erfolgen und abgelegt werden. Informationen, die nach dem Entschied nicht mehr wichtig sind, sollten umgehend gelöscht werden. Falls eine Sicherheitsüberprüfung mit einer externen Stelle gemacht wird, muss die Einhaltung des Datenschutzes beim Austausch mit der externen Stelle und bei der Ablage geprüft und dokumentiert sein.
- **Mitarbeitendenverzeichnis:** Ein Mitarbeitendenverzeichnis sollte zeigen, wer aufgrund seiner Aufgaben, Zutrittsberechtigungen und Rollen geprüft werden muss, sowie ob diese Prüfung stattgefunden hat. Ob eine Prüfung notwendig ist, hängt vor allem von der Kritikalität der Aufgaben sowie der Schäden ab, welche diese Person dem Unternehmen zufügen könnte.
- **Externe Liefernde:** Mitarbeitende von externen Liefernden müssen mit einbezogen werden und vertraglich zu Sicherheitsüberprüfungen verpflichtet werden können (eine fehlende Verpflichtung zu solchen Prüfungen sollte im Risikomanagement dokumentiert werden).

4 Abkürzungen

BACS Bundesamt für Cybersicherheit
BFE Bundesamt für Energie
BWL Bundesamt für wirtschaftliche Landesversorgung
CSF Cyber Security Framework
ISG Informationssicherheitsgesetz

ISO Internationale Organisation für Normung
NIST National Institute of Standards and Technology
VBS Eidgenössisches Departement Verteidigung, Bevölkerungsschutz und Sport