/SSS information security society switzerland

Positionspapier: Aufbau eines Vulnerability Radars für die Schweiz

Einleitung: Vulnerability Management spielt eine entscheidende Rolle im Schutz vor Cyberbedrohungen, insbesondere in einer zunehmend digitalisierten Welt. Die Schweiz als internationale Drehscheibe für Innovation, Wirtschaft und Technologie ist besonders gefährdet und muss sich proaktiv mit diesem Thema auseinandersetzen. Nachdem im neuen Informationssicherheitsgesetz die Meldepflicht von Schwachstellen bei Kritischen Infrastrukturen abgelehnt wurde, skizziert dieses Positionspapier die Notwendigkeit eines Vulnerability Radars für kritische Infrastrukturen in der Schweiz**.** Der Charakter hinsichtlich Meldung von Vulnerabilities basiert dabei auf Freiwilligkeit.

I. Herausforderungen:

- **Verwundbarkeiten in IT-Infrastruktur**: Kritische Sektoren wie z.B. Energieversorgung, Gesundheitswesen und Finanzdienstleistungen sind anfällig für Cyberangriffe, die erhebliche Auswirkungen auf die Gesellschaft haben können. Es wäre im Interesse von Allen, wenn entsprechende Schwachstellen anonym und sicher gemeldet werden könnten und die Informationen der Wirtschaft breit zur Verfügung stehen würden.

- **Keine Verpflichtung**: Die Betreiber kritischer Infrastrukturen haben momentan keine Pflicht, ihre Schwachstellen zu melden. Es muss ein Umfeld geschaffen werden, damit dies freiwillig geschieht. Hierzu gehört auch, dass der Unternehmensführung und anderen verantwortlichen Organen wie z.B. Verwaltungsräten bewusst gemacht wird, dass sie ihren Verpflichtungen im Kontext des Risikomanagements nachkommen.

II. Empfehlungen:

- **Aufbau eines nationalen Vulnerability Radars***:* Die Schweiz soll eine nationale Plattform für das Vulnerability Management einführen, das branchenübergreifende Standards, Prozesse und Richtlinien festlegt. Dies fördert die Zusammenarbeit zwischen Regierung sowie Unternehmen. Die Meldungen erfolgen im Sinne der partizipativen Sicherheit auf freiwilliger Basis von den betroffenen Unternehmen. Damit profitieren alle Unternehmen und sorgen für ein Stück mehr Cybersicherheit in der Schweiz.

- **Cyber Security Hub als Plattform***:* Ein effektiver Vulnerability Radar erfordert einen kontinuierlichen Informationsaustausch über Bedrohungen und Schwachstellen. Diese Schwachstellen sollen möglichst einfach und anonym gemeldet werden können. Das Bundesamt für Cyber Sicherheit (BACS) könnte hier mit der bereits bestehenden Plattform “Cyber Security Hub (CSH)” ein entsprechendes Gefäss, zur Meldung solcher Schwachstellen zur Verfügung stellen.

- **Mehrwert des Vulnerability Radars**: Die Herausforderung, welcher ein Unternehmen im Umgang mit Verwundbarkeiten gegenübersteht, besteht insbesondere aus der

grossen Anzahl an Informationen zu Verwundbarkeiten (z.B. Known Exploited Vulnerabilities Catalog – CVEs[1]). Das BACS stellt neben CSH-Plattform insbesondere die Tätigkeit der Priorisierung sicher und publiziert die aktuell in der der Schweiz relevantesten Vulnerabilities. Durch diese Triage und Zurverfügungstellung der Vulnerabilities bietet das BACS mit dem CSH der Schweiz eine weitere Massnahme, um ihre Wirtschaft vor Cyberangriffe zu schützen.

- **Ausbau der Ausbildungs- und Sensibilisierungsmassnahmen***:* Um eine nachhaltige Verbesserung der Sicherheitskultur zu erreichen, sollte verstärkt in Schulungen und Sensibilisierungsmassnahmen für die verantwortlichen Personen (insbesondere verantwortliche Organe in Unternehmen und Organisationen) investiert werden.

Fazit: Ein effektiver Vulnerability Radar ist von entscheidender Bedeutung, um die digitale Infrastruktur der Schweiz vor Cyberbedrohungen zu schützen. Die Idee einer nationalen Plattform für Schwachstellen (beispielsweise via dem bereits bestehenden Cyber Security Hub des BACS) soll weiterverfolgt werden und die hierfür nötigen Ressourcen bereitgestellt werden. Eine solche Plattform würde sich ebenfalls mit der Massnahme 5 der Nationalen Cyberstrategie vereinbaren lassen.

Mit freundlichen Grüssen

Dario Walder

ISSS Vize Präsident
Information Security Society Switzerland (ISSS)
Zentweg 13
3006 Bern
E-Mail: vicepresident@isss.ch

[1] https://www.cisa.gov/known-exploited-vulnerabilities-catalog