Dialog für Cybersicherheit

Ideen-Skizze im Dialog für Cybersicherheit

Arbeitstitel/Thema	Cyberdome

Problem-/Fragestellung inkl. Bezug zur IT-/Cybersicherheit	Gesamtgesellschaftliche Relevanz
Threat Intelligence Informationen zu Cyberangriffen sind oftmals in Expertenkreisen bekannt, landen aber nicht bei den zuständen Stellen in der öffentlichen Hand, in Unternehmen oder in der Zivilgesellschaft. Oftmals werden Behörden und Unternehmen unnötig Opfer von Cyberangriffen, da seit einigen Tagen / Stunden bekannte C2-Domains und C2-IP-Adressen weder gefiltert noch blockiert wurden.	Große Schäden in Staat, Wirtschaft und Zivilgesellschaft durch Cybercrime.

Mögliche Herangehensweise
- Das BSI betreibt mit dem ITZBund eigene DNS--Server für die öffentliche Verwaltung, die aktiv und 24/7 aktuelle Threat Intel abbilden und entsprechende Domains blockieren und Alarmmeldungen auslösen. Die Nutzung durch die öffentliche Hand ist zunächst freiwillig, könnte aber über regulatorische Änderungen auch erzwungen werden. - Das BSI kooperiert mit deutschen ISPs, damit diese ihre Behörden- und Businesskunden mit IP- und Domainfilter auf Basis einer aktuellen Sperrliste aktiv verteidigen. Diese sollte für die Endkunden nicht prohibitiv teuer sein, transparent und per Opt-In erfolgen.

Zielgruppe(n)	Geschätzte Laufzeit
Staat Wirtschaft Zivilgesellschaft	mehr als 6 Monate

Angestrebte Ergebnisse	Diskussionspunkte / Offene Fragen / ggf. weitere Stakeholder
- kuratierter Threat-Intel-Feed für Domains und IP-Adressen - DNS-Server für öffentliche Hand - gemeinsames Marketing mit ISPs ("Opt-In Cyberdome-Option für ihren Internetanschluss") - ISPs bieten Schutzoption an	ISPs / ECO e.V.