|  |  |
| --- | --- |
| Name des Vorfalls: | Stuxnet 2010 |
| Durchführende/r: | *Wer/Welche Gruppe hat den Vorfall durchgeführt?*  *Informationen zu der Gruppe/Person mit klassischen Eckdaten: Wer, persönlicher Hintergrund, Land*  *z.Bsp. Unbekannte Hacker (SO1) .. SO1 Literaturhinweis von unten!!*  Die Auftraggeber von Stuxnet werden meist in Israel und den USA vermutet. Dies beruht jedoch nur auf Annahmen und Aussagen einzelner Personen. Offizielle Bestätigungen oder Geständnisse seitens der Regierungen liegen nicht vor (SO1, SO2). Klar ist jedoch, dass hinter dem Computerwurm viele Entwickler standen, die mehrere Jahre daran gearbeitet haben (SO4, SO3). Das Ziel des Angriffes waren vermutlich iranische Atomanlagen (SO2). Die Auftraggeber wollten damit wahrscheinlich einen Krieg zwischen Israel und Iran verhindern, indem sie die Uranproduktion sabotierten (SO3). Da jedoch auch viele andere von dem Wurm betroffen waren, könnte es sich ebenso um einen allgemeinen Test zur Manipulation von Industrieanlagen gehandelt haben (SO2). |
| Wer hat den Vorfall entdeckt: | *Informationen zu der Gruppe/Person mit klassischen Eckdaten: Wer, persönlicher Hintergrund, Land*  Stuxnet wurde erstmals in einem iranischen Bürogebäude bemerkt, nachdem Mitarbeiter wiederholt Ausfälle und Blue-Screens ihrer PCs gemeldet hatten. Schließlich entdeckten Sergey Ulasen und sein Team aus Belarus den Wurm, nachdem sie für einen iranischen Kunden die PCs untersuchten (SO3, SO4). |
| Beschreibung | Exakte Beschreibung des Vorfalls mit detaillierten Informationen:  **Wie wurde die Attacke durchgeführt?**  Stuxnet war ein Computerwurm, der sich selbst verbreiten konnte – über USB-Sticks und Netzwerke. Er nutzte Sicherheitslücken in Windows und manipulierte Siemens-Steuerungssoftware, sodass Zentrifugen von Urananreicherungsanlagen in Iran beschädigt wurden, ohne dass es die Betreiber merkten (SO2, SO3).  **Welche Gegenmaßnahmen wurden durchgeführt durch wen?**  Antivirenfirmen analysierten den Computerwurm, Siemens und Microsoft veröffentlichten Updates, und Anlagenbetreiber sperrten USB-Sticks, trennten Netzwerke und überprüften ihre Systeme (SO2, SO4).  **Welche Personen waren von dem Vorfall betroffen?**  Vor allem iranische Urananreicherungsanlagen, keine direkten Personenverletzungen, aber viele technische Probleme für die Mitarbeiter (SO2, SO3). Jedoch wurden Weltweit PCs infiziert, wobei meist jedoch kein Schaden entstand (SO2).  **Aktuelle Status des Hacks im Jahr 2025!**  Stuxnet selbst kann heute keinen Schaden mehr anrichten, weil die Sicherheitslücken geschlossen wurden. Die Technik des Virus diente späteren Cyberangriffen als Vorlage (SO2, SO5). |
| Schadenssumme: | Eine genaue Schadenssumme ist nicht bekannt, da viele Informationen geheim gehalten werden, könnte sich jedoch auf mehrere hundert Millionen Euro belaufen. Sicher ist, dass 2009 die Produktionskapazität einer iranischen Atomanlage um etwa 15 % gesunken ist, vermutlich verursacht durch Stuxnet (SO2). |
| Literaturhinweise | *Woher stammen die Informationen und in welchen Bereichen wurden sie eingesetzt*  *z.B.*  *SO1,* [*https://www.trellix.com/de-de/security-awareness/ransomware/what-is-stuxnet/*](https://www.trellix.com/de-de/security-awareness/ransomware/what-is-stuxnet/)  *SO2,* [*https://de.wikipedia.org/wiki/Stuxnet*](https://de.wikipedia.org/wiki/Stuxnet)  *SO3,* [*https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html*](https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html)  *SO4,* [*https://www.bmlv.gv.at/truppendienst/ausgaben/artikel.php?id=1119*](https://www.bmlv.gv.at/truppendienst/ausgaben/artikel.php?id=1119)  *SO5,* [*https://www.stormshield.com/de/news/stuxnet-welche-lehren-lassen-sich-zwoelf-jahre-spaeter-ziehen/*](https://www.stormshield.com/de/news/stuxnet-welche-lehren-lassen-sich-zwoelf-jahre-spaeter-ziehen/)   * *Mindestens fünf unterschiedliche Literaturhinweise mit dem Hinweis der Verwendung im Text!.* |