Konzept für softwarebasierte technische Überwachungsgeräte

Studiengang: MAS Digital Forensics & Cyber Investigation

Seit 2020 verzeichnet das Bundesamt für Statistik einen Anstieg digitaler Straftaten um 36.74% bis 2022, mit einer Aufklärungsquote von nur 34.3% im selben Jahr. Eine Herausforderung für Strafverfolgungsbehörden besteht in der wachsenden Nutzung von Verschlüsselungstechniken. Ein jüngstes Bundesgerichtsurteil vom 9. Februar 2022 bestätigt die Zulässigkeit von Keylogger-Software gemäss Artikel 280 der Schweizerischen Strafprozessordnung.

Ausgangslage

Das Bundesamt für Statistik verzeichnet seit 2020 einen starken Anstieg digitaler Straftaten. Von 24‘398 Fällen in 2020 stiegen die Fälle auf 33‘345 im Jahr 2022, was einen Anstieg von 36.74% darstellt. Es ist jedoch zu betonen, dass viele Straftaten nicht gemeldet werden, was auf eine hohe Dunkelziffer hinweist. Zudem unterstreicht das Bundesamt, dass diese Zahlen mit Vorsicht zu interpretieren sind, da neue Phänomene auftauchen und in die Statistik einfliessen könnten. Cyberkriminalität ist weltweit ein wachsendes Problem, wobei Prognosen die durch Cyberkriminalität verursachten Kosten bis 2025 auf 10.5 Billionen US-Dollar schätzen. Ein Grossteil der Straftaten bleibt ungeklärt, mit einer Aufklärungsquote von nur 34.3% bis 2022. Die globalisierte Vernetzung und verschiedene Gesetzgebungen in verschiedenen Ländern erschweren die Strafverfolgung. Technische Hilfsmittel, insbesondere Verschlüsselungen, stellen zudem ein Hindernis für die Strafverfolgung dar. Die Digitale Forensik stösst hierbei, insbesondere bei der Entschlüsselung von Datenträgern, an ihre Grenzen. Es ist von entscheidender Bedeutung, effektive Methoden zur Überwindung solcher Verschlüsselungen zu entwickeln.

Zielsetzung und Vorgehen

Die Arbeit konzentriert sich auf die Rahmenbedingungen für den Einsatz von Keyloggern und die Entwicklung eines modularen, softwarebasierten Prototypen, der Tastatureingaben und Bildschirmaufnahmen aufzeichnet. Um ein umfassendes Verständnis der Technologien und Herausforderungen rund um Keylogger zu gewinnen, wurde eine tiefgehende Literaturrecherche durchgeführt. Diese Recherche zeigt die diversen Technologien, die in der aktuellen Keylogger-Landschaft verwendet werden und ermöglicht einen detaillierten Vergleich der Technologien. Aus dieser Analyse heraus wurden insgesamt acht unterschiedliche User- und Kernel-Keylogger-Methodiken sorgfältig untersucht. Neben der technischen Analyse wurde ein besonderer Fokus auf die rechtlichen Aspekte gelegt. Durch die Würdigung der Gesetzgebung und des relevanten Bundesgerichtsentscheids konnte ein solides Fundament für die Implementierung und den Vergleich der Prototypen geschaffen werden, wobei stets darauf geachtet wurde, dass diese im Einklang mit den geltenden Gesetzen stehen.

Ergebnisse

Die intensive Forschung und Entwicklung führten zur erfolgreichen Erstellung mehrerer Keylogger-Prototypen. Durch sorgfältige Tests und Evaluierungen konnten wertvolle Erkenntnisse bezüglich der Performance und Erkennungsraten der verschiedenen Prototypen gesammelt werden. Dies ermöglichte nicht nur eine fundierte Einschätzung ihrer Wirksamkeit und Effizienz, sondern auch eine Analyse potenzieller Schwachstellen. Darüber hinaus wurde, basierend auf den gewonnenen Erkenntnissen, eine umfassende Prozess-Pipeline entwickelt. Diese Pipeline ist speziell darauf ausgelegt, von Strafverfolgungsbehörden genutzt zu werden und bietet eine strukturierte und effiziente Methode zur Datenerfassung, -analyse und -übermittlung, um Cyberkriminalität effektiv zu bekämpfen.

Sebastian Peyer