Cellebrite

WHITEPAPER

Technologie zur Bekämpfung der Ausbeutung von Kindern im Internet

VON JARED BARNHART
Cellebrite

Die digitale Landschaft der Ausbeutung von Kindern: Eine wachsende Krise

Das digitale Zeitalter stellt weiterhin eine große Herausforderung für den Schutz von Kindern im Internet dar. Im Jahr 2024 gingen bei der CyberTipline des National Center for Missing & Exploited Children (NCMEC) 20,5 Millionen Meldungen über mutmaßliche sexuelle Ausbeutung von Kindern ein. Dies scheint zwar ein deutlicher Rückgang gegenüber den 36,2 Millionen Meldungen im Jahr 2023 zu sein, jedoch ist die tatsächliche Zahl
Die Anzahl der gemeldeten Vorfälle belief sich auf 29,2 Millionen, was vor allem auf eine neue Bündelfunktion zurückzuführen ist, die verwandte Meldungen zusammenfasst – was deutlich macht, dass das Ausmaß des Missbrauchs weiterhin alarmierend hoch ist. [1]

Diese Krise ist weltweit zu beobachten, da illegale Bilder leicht über das Internet verbreitet werden können. Weltweit hat die Internet Watch Foundation (IWF) in ihrem Jahresbericht 2024 „Annual Data and Insights Report" angegeben, dass sie über 424.000 Meldungen von URLs mit Material über sexuellen Kindesmissbrauch (CSAM) geprüft hat – das entspricht einer Meldung alle 74 Sekunden. Von diesen wurden 96 % als CSAM bestätigt und 81 % wurden in Europa gehostet. Die IWF stellte außerdem einen besorgniserregenden Anstieg selbst erstellter Inhalte fest: Jede zweite Webseite enthielt Material, das von Kindern selbst erstellt worden war, oft unter Zwang oder Manipulation.

Da Täter zunehmend digitale Plattformen nutzen, um Kinder zu manipulieren, auszubeuten und illegale Inhalte zu verbreiten, müssen Strafverfolgungsbehörden digitale Ermittlungslösungen einsetzen, um diese Verbrechen wirksam zu bekämpfen. Die schiere Menge an CyberTips- und IWF-Meldungen hat viele Task Forces zur Bekämpfung von Internetkriminalität gegen Kinder (ICAC) überfordert, die oft über zu wenige Ressourcen und zu wenig Personal verfügen.

Diese Flut an digitalen forensischen Beweisen stellt eine doppelte Herausforderung dar: die Priorisierung von Ermittlungen bei gleichzeitiger Verwaltung riesiger Datenmengen. Es gibt jedoch auch einen Lichtblick. Fälle von Straftaten gegen Kinder werden oft stark mediatisiert und mit strengen Strafen für die Täter geahndet. Bei erfolgreicher Strafverfolgung bieten diese Fälle den Leitern der Behörden eine hervorragende Gelegenheit, ihre Wirksamkeit unter Beweis zu stellen, das Vertrauen der Bevölkerung wiederherzustellen und die entscheidende Rolle der Behörden für die öffentliche Sicherheit beim Schutz der Schwächsten zu bekräftigen.

DIGITALE BEWEISE – DER SCHLÜSSEL ZU ERFOLGREICHEN STRAFVERFOLGUNGEN

Digitale Intelligenz bezieht sich auf die rechtmäßige Erfassung, Analyse und Anwendung von Daten aus digitalen Quellen – wie Mobiltelefonen, Computern, sozialen Medien und Cloud-Plattformen –, um Ermittlungsergebnisse zu erzielen. In Fällen von Internetkriminalität gegen Kinder (ICAC) ist diese Intelligenz oft der Dreh- und Angelpunkt für eine erfolgreiche Strafverfolgung.

Die langjährige Partnerschaft zwischen Cellebrite und dem National Center for Missing and Exploited Children (NCMEC) hat mit der Integration der Hash-Wert-Liste der CyberTipline des NCMEC in Cellebrite Inseyets einen bedeutenden Schritt nach vorne gemacht. Diese Weiterentwicklung soll Ermittlungen bei Straftaten gegen Kinder beschleunigen, indem sie den Strafverfolgungsbehörden sofortigen Zugriff auf bekanntes Material über sexuellen Kindesmissbrauch (CSAM) ermöglicht und die Zeit bis zur Beweisaufnahme und Gerechtigkeit für die Opfer verkürzt.

- Die Hash-Werteliste der CyberTipline des NCMEC, die etwa 10 Millionen bekannte CSAM-Dateien enthält, ist nun in Cellebrite Inseyets integriert und ermöglicht die sofortige Identifizierung illegaler Dateien auf verdächtigen Geräten.
- Diese Integration ermöglicht es Ermittlern, CSAM-Dateien schnell abzugleichen und die Exposition gegenüber schädlichen Inhalten zu reduzieren, was die psychische Gesundheit von Prüfern oder Ermittlern unterstützt – und gleichzeitig Festnahmen und Strafverfolgungen beschleunigt.

Die schnelle Identifizierung von CSAM spielt eine entscheidende Rolle bei der Entfernung missbräuchlicher Inhalte aus dem Umlauf. Ermittler können elektronische Dienstleister (ESP) zur Entfernung benachrichtigen, sich an das Child Victim Identification Program (CVIP) des NCMEC wenden, um zur Identifizierung unbekannter Opfer beizutragen und dazu beizutragen, die erneute Viktimisierung von Kindern zu verhindern. Für die Opfer und ihre Familien können diese Bemühungen ein gewisses Maß an Gerechtigkeit und Heilung bringen.

Investigative Analysetools können diesen Prozess optimieren, indem sie:

- Daten aus verschiedenen Quellen auf einer einheitlichen Plattform konsolidieren.
- Maschinelles Lernen zur Identifizierung relevanter Medien-, Kommunikations- und Geolokalisierungsdaten einsetzen.
- die Zusammenarbeit zwischen Behörden durch den effizienten Austausch von Erkenntnissen und Beweisen zu erleichtern.
- Solche Funktionen beschleunigen nicht nur die Ermittlungen, sondern stellen auch sicher, dass Strafverfolgungen durch solide, zulässige digitale Beweise gestützt werden.

LÖSUNGEN FÜR FINANZIERUNGSPROBLEME

Task-Force-Programm: Finanzierungsstrategien in den USA, Europa und im asiatisch-pazifischen Raum

In den Vereinigten Staaten erhielt das Task Force-Programm „Internet Crimes Against Children" (ICAC) im Geschäftsjahr 2023 ein Budget von 40,8 Millionen US-Dollar zur Unterstützung von 61 koordinierten Task Forces und über 5.400 Strafverfolgungsbeamten auf Bundes-, Landes- und lokaler Ebene Diese Finanzierung stellt eine erhebliche Steigerung gegenüber den 31,2 Millionen US-Dollar im Geschäftsjahr 2022 dar und unterstreicht das wachsende Engagement im Kampf gegen die Ausbeutung von Kindern im Internet. Die angeschlossenen Behörden profitieren von Mitteln, die für Schulungen und Beratungsleistungen bereitgestellt werden. Weitere Finanzierungsmöglichkeiten sind die Einziehung von Vermögenswerten, Partnerschaften mit der Electronic Crimes Task Force des US-Geheimdienstes und Kooperationen mit Partnerbehörden. Der Einsatz digitaler Intelligence-Tools kann die Aufklärung von Fällen beschleunigen, was möglicherweise zu einer erhöhten Einziehung von Vermögenswerten und weiteren Finanzierungsmöglichkeiten führt.

In Europa hat der Fonds für die innere Sicherheit (ISF) der Europäischen Union für den Zeitraum 2021–2027 1,93 Milliarden Euro bereitgestellt, um die Sicherheit innerhalb der EU durch die Prävention und Bekämpfung von schwerer und organisierter Kriminalität, einschließlich Cyberkriminalität, zu verbessern. Dieser Fonds unterstützt Strafverfolgungsbehörden bei der Einführung fortschrittlicher Technologien und Methoden zur Bekämpfung von Straftaten gegen Kinder.

In der Region Asien-Pazifik hat Thailand im Rahmen des Kinderschutzgesetzes von 2003 einen Kinderschutzfonds eingerichtet, der vom Ministerium für soziale Entwicklung, Abteilung für Kinder und Jugendliche (DCY), verwaltet wird. Dieser Fonds stellt Mittel für die Unterstützung, den Sozialschutz und die Verhaltensförderung von Kindern und Familien sowie von Verwandten und Pflegefamilien bereit.

Australien hat durch verschiedene Finanzierungsinitiativen sein Engagement für den Kinderschutz unter Beweis gestellt. So wurden beispielsweise im Staatshaushalt 2023–24 von Südaustralien 216,6 Millionen Dollar für das Kinderschutzsystem des Bundesstaates bereitgestellt, um Maßnahmen zur Deckung der Kosten für Kinder in Pflege zu finanzieren und neue Maßnahmen zur Unterstützung des Systems einzuführen. [4]

Trotz dieser erheblichen Investitionen sehen sich viele ICAC-Einheiten und ihre Pendants weltweit mit

Budgetbeschränkungen konfrontiert, die die Einführung modernster digitaler Intelligence-Tools behindern. Um dieser Herausforderung zu begegnen:

- Bundes- und Landeszuschüsse: Bereitstellung spezieller Mittel zur Ausstattung der ICAC-Einheiten mit den erforderlichen Technologien.
- Öffentlich-private Partnerschaften: Zusammenarbeit mit Technologieunternehmen, um Zugang zu Tools und Schulungsressourcen zu erhalten.
- Gesetzgeberische Unterstützung: Verabschiedung von Gesetzen, die den Einsatz digitaler Ermittlungsmethoden in Fällen von Kindesmissbrauch vorschreiben und finanzieren.

Investitionen in diesen Bereichen stellen sicher, dass die ICAC-Einheiten nicht von den sich weiterentwickelnden Taktiken der Straftäter überholt werden.

20,5 Mio.
Meldungen gingen 2024 bei der NCMEC CyberTipline ein

546
Meldungen, die 2024 beim NCMEC zu Online-Verführung eingegangen sind

91
Gesamtzahl der dem NCMEC im Jahr 2024 gemeldeten Fälle von vermissten Kindern

„Wir haben verstanden, warum es während der Pandemie zu Kindesmissbrauch kam – da Kinder ständig online waren –, aber warum er nicht zurückging, war wirklich rätselhaft. Dann haben wir bedacht, dass jeden Tag mehr und mehr Apps entwickelt werden und immer mehr Kinder Zugang zu einem Gerät haben. Kinder erstellen sogar ihre eigenen expliziten Inhalte und laden sie hoch – sie finden das lustig oder cool und sind sich nicht bewusst, was sie tun."

-Leutnant Eric Kinsman, Leiter der Task Force „Internet Crimes Against Children" (ICAC) in New Hampshire

WIE DIGITALE BEWEISE ERMITTLERN BEI DER BEKÄMPFUNG DER ONLINE-AUSBEUTUNG VON KINDERN HELFEN:

Die Implementierung digitaler Intelligence-Tools und die Modernisierung der Ermittlungsabläufe bieten den ICAC-Einheiten konkrete, unmittelbare Vorteile. Diese Funktionen rationalisieren die Ermittlungen, reduzieren Rückstände und beschleunigen die Identifizierung und den Schutz der betroffenen Kinder.

1. Umfassende und rechtmäßige Datenerfassung

- Sammeln Sie Daten von einer Vielzahl von Geräten, die von Straftätern verwendet werden, an nahezu jedem Ort – am Tatort, in Fahrzeugen, in einem Kinderhilfezentrum oder im Labor.
- Greifen Sie auf gesperrte iOS- und Android-Geräte zu und erschließen Sie bisher nicht verfügbare Beweise, die für die Aufklärung von Fällen entscheidend sind.
- Extrahieren und betrachten Sie Daten aus sicheren und verschlüsselten Chat-Anwendungen, einschließlich der Möglichkeit, Screenshots von nicht unterstützten Plattformen zu erstellen und diese in Fallberichte zu integrieren.

2. Erweiterte Analysefunktionen

- Nutzen Sie KI, um Ermittlungsansätze zu identifizieren, indem Sie Daten aus mehreren digitalen Quellen filtern, verknüpfen und visualisieren.

- Identifizieren Sie Muster und finden Sie wichtige Beweise schneller, um zu verhindern, dass Verbindungen zwischen Opfern, Tätern und digitalen Artefakten übersehen werden.

3. Verbesserte Berichterstattung und Opferschutz

- Erstellen Sie maßgeschneiderte, leicht lesbare Berichte für Staatsanwälte, Partner und Interessengruppen mit Filtern, die sicherstellen, dass nur wesentliche Falldaten weitergegeben werden.
- Entfernen Sie automatisch Bilder von Kindesmissbrauch aus Berichten, um den Schaden für die Opfer zu verringern und eine Überlastung der Ermittler zu verhindern.
- Schaffen Sie Vertrauen in der Öffentlichkeit, indem Sie einen umsichtigen und datenschutzbewussten Umgang mit sensiblen digitalen Beweismitteln demonstrieren.

4. Sichere Zusammenarbeit und Fallmanagement

- Teilen und hosten Sie gesammelte Daten in Echtzeit über sichere Plattformen – ohne Abhängigkeit von physischen Medien und unter Wahrung der Beweiskette
- Bereiten Sie sich auf Einsätze vor, indem Sie Open-Source-Informationen nutzen, um potenzielle Straftäter zu identifizieren, und exportieren Sie Informationen nahtlos in Fallmanagementsysteme.
- Sicherstellung der behördenübergreifenden Koordination mit Fallakten, die mit NCMEC-, Project VIC- und CAID-Hash-Sets kompatibel sind, um die Identifizierung von Opfern zu beschleunigen.

5. Skalierbarkeit über ICAC-Fälle hinaus

- Wenden Sie digitale Intelligence-Workflows auf eine Vielzahl von Fällen an, die über die Ausbeutung von Kindern hinausgehen, darunter Mord, Gewaltverbrechen, Drogenhandel und Wirtschaftskriminalität, um den Wert der Investitionen der ICAC in diese Tools zu maximieren.

6. Beschleunigung der Justiz durch die Integration von Cellebrite und NCMEC

- Sofortige Erkennung von CSAM: Cellebrite Inseyets integriert nun die Hash-Wert-Liste der CyberTipline des NCMEC – etwa 10 Millionen bestätigte CSAM-Dateien – und ermöglicht so die sofortige Identifizierung von bekanntem Material auf verdächtigen Geräten.

Diese Funktionen verbessern nicht nur die Ermittlungsergebnisse, sondern reduzieren auch die emotionale Belastung der Ermittler, indem sie die Konfrontation mit verstörenden Inhalten minimieren.

Der Kampf gegen Internetkriminalität, die sich gegen Kinder richtet, ist ein Wettlauf mit der sich rasant entwickelnden Technologie. Durch den Einsatz digitaler Intelligenz können Strafverfolgungsbehörden einen Vorsprung behalten und sicherstellen, dass Täter vor Gericht gestellt werden und Opfer den Schutz erhalten, den sie verdienen. Es ist unerlässlich, dass alle Beteiligten auf allen Ebenen die Bedeutung dieser Instrumente erkennen und sich dafür einsetzen, ihre Integration in die Arbeit der ICAC zu unterstützen.

Lesen Sie, wie die Polizei von Glastonbury die Digital Intelligence Platform von Cellebrite einsetzte, um einen Verdächtigen in einem wichtigen Fall von Kindesmissbrauch vor Gericht zu bringen. Um mehr darüber zu erfahren, wie die Digital Intelligence Platform von Cellebrite Ihrer ICAC-Einheit dabei helfen kann, mehr Fälle schneller aufzuklären, besuchen Sie bittewww.celebrite.com/contact .

Über Cellebrite

Die Mission von Cellebrite (Nasdaq: CLBT) besteht darin, seinen Kunden zu ermöglichen, Leben zu schützen und zu retten, die Justiz zu beschleunigen und die Privatsphäre in Gemeinschaften auf der ganzen Welt zu wahren. Wir sind ein weltweit führender Anbieter von Digital Intelligence-Lösungen für den öffentlichen und privaten Sektor und unterstützen Organisationen dabei, die Komplexität gesetzlich sanktionierter digitaler Ermittlungen durch die Optimierung von Intelligence-Prozessen zu bewältigen. Die digitale Informationsplattform und die Lösungen von Cellebrite genießen das Vertrauen Tausender führender Behörden und Unternehmen weltweit und verändern die Art und Weise, wie Kunden Daten in gesetzlich sanktionierten Ermittlungen sammeln, überprüfen, analysieren und verwalten.

- Weitere Informationen finden Sie unter www.cellebrite.com
- Kontaktieren Sie Cellebrite weltweit unter www.cellebrite.com/contact

Cellebrite