POLICE

SPI-Kolloquium 01.02.2024

Herausforderungen in der Bekämpfung der Cyberkriminalität

Was ist Cyberkriminalität

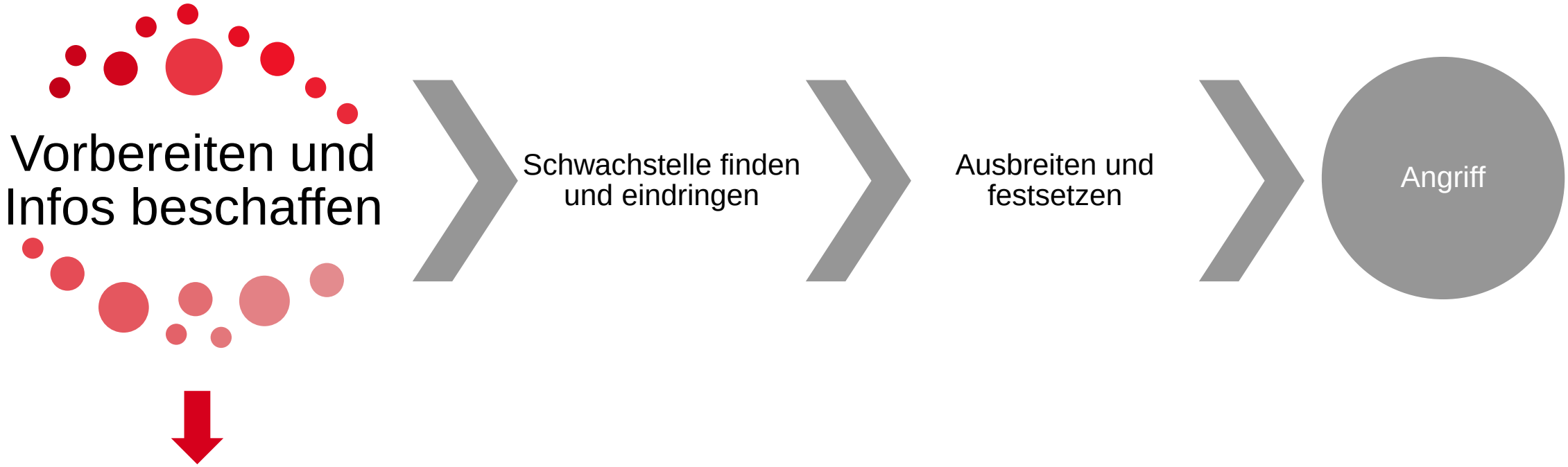
- Der Begriff "Cyberkriminalität" umfasst sämtliche strafrechtlichen Handlungen und Straftaten im Cyberspace, die vom fedpol als Phänomene der Cyberkriminalität erfasst wurden.

- Innerhalb dieser Deliktsklasse erfolgt eine Differenzierung, ob eine Straftat durch Nutzung (digitalisierte Kriminalität) oder gegen die Informations- und Kommunikationstechnik (Cybercrime) begangen wurde.

- Delikte wie Cyberbetrug, Sextortion, Grooming, rufschädigende Kommentare usw., die bisher hauptsächlich in der realen Welt begangen wurden, werden aufgrund der zunehmenden Nutzung der Informations- und Kommunikationstechnik der digitalisierten Kriminalität zugeordnet.

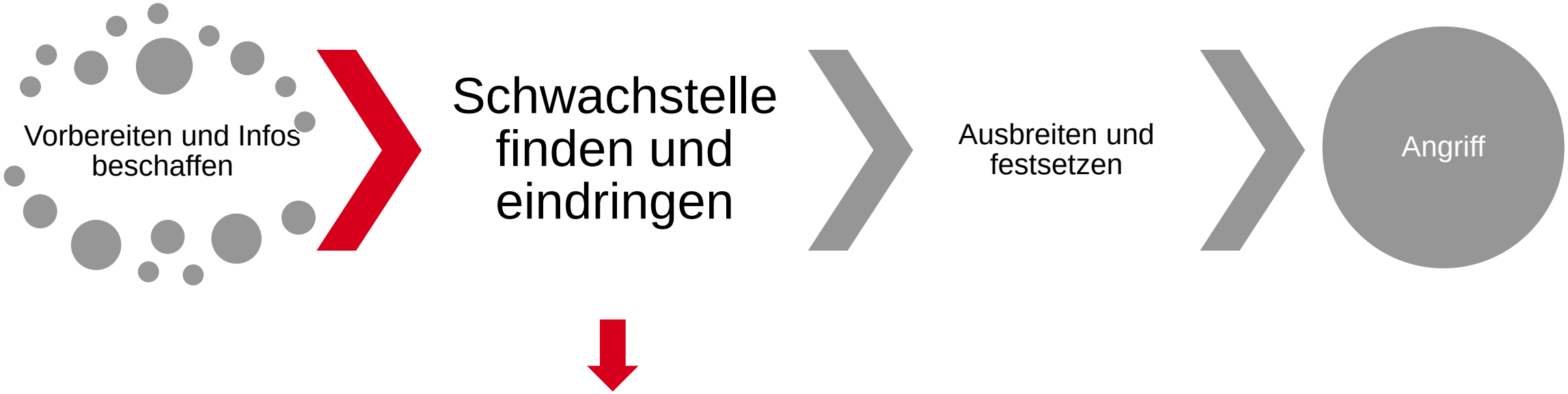
- **Cybercrime-Delikte wie beispielsweise Hacking, Malware (Ransomware) usw. richten sich explizit gegen die Informations- und Kommunikationstechnik (Cybercrime) und folgen in der Regel nachfolgendem Vorgehen:**

Häufiges Vorgehen (grob)



z. B. Webseiten, Soziale Medien, Darknet, Spear-Phishing, betrügerische Anrufe, Schadsoftware

Häufiges Vorgehen (grob)

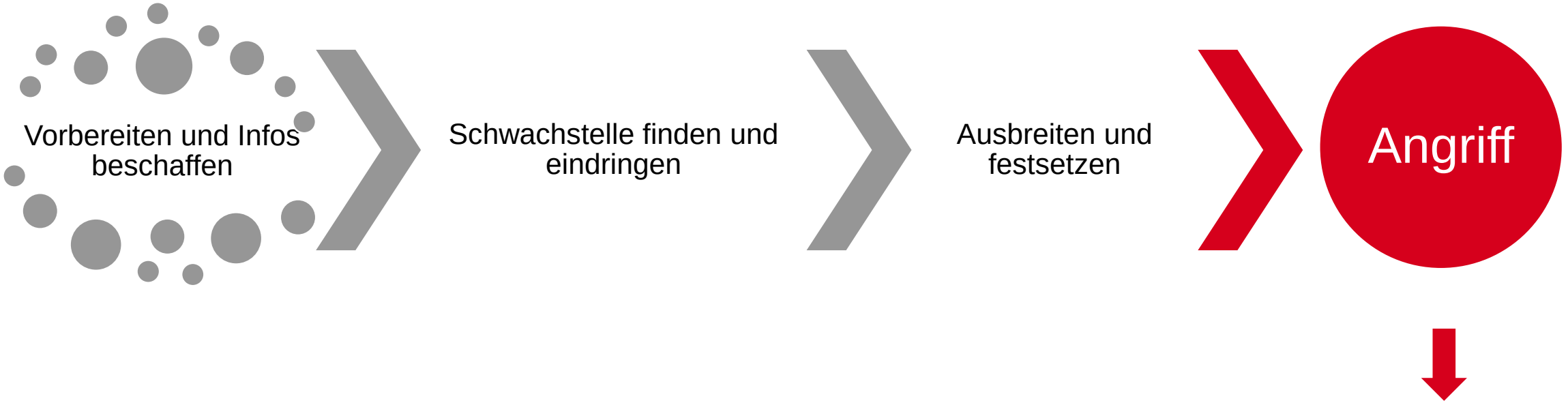


z. B. mithilfe von gestohlenen Daten, Schadsoftware, Sicherheitslücken

Häufiges Vorgehen (grob)

z. B. sensible Daten suchen, Datenmanipulation

Häufiges Vorgehen (grob)



z. B. Verschlüsselung oder Datenabfluss

Aufgaben: Forensischen Informatik mit dem Schwerpunkt Cybercrime

- Entwicklung neuer Ermittlungs- und Untersuchungsmethoden sowie Kenntnisse über deren praktische Anwendungen.
- Untersuchung von Informatik-Systemen unter Beachtung forensischer und rechtlicher Grundsätze.
- Untersuchung von Cyber-Vorfällen (Incident Response) und unterstützen des Opfers bei der Gefahrenabwehr.
- Unterstützung und Begleitung des Ermittlers bei der Analyse und Interpretation von digitalen Beweisen.
- Erstellen detaillierter Untersuchungsberichte, Ermittlungs- und Präventionsempfehlungen.

Kompetenzprofil: Forensischen Informatik mit dem Schwerpunkt Cybercrime

- **Fachkenntnisse in forensischer Informatik:**
  - Entwicklung neuer Ermittlungs- und Untersuchungsmethoden sowie Kenntnisse über deren praktische Anwendungen.
  - Umfassende Erfahrung in der forensischen Untersuchung von Informatik-Systemen, unter Beachtung forensischer Grundsätze.
- **Cyber-Sicherheit und Incident Response:**
  - Expertise in der Untersuchung von Cyber-Vorfällen (Incident Response).
  - Fähigkeit zur Unterstützung von Opfern bei der Abwehr von Gefahren (Gefahrenabwehr)
- **Analytische Fähigkeiten:**
  - Unterstützung und Begleitung von Ermittlern bei der Analyse und Interpretation von digitalen Beweisen.
  - Kompetenz in der Durchführung von Ermittlungen unter Berücksichtigung rechtlicher und ethischer Aspekte.
- **Berichterstellung und Empfehlungen:**
  - Erfahrung in der Erstellung detaillierter Untersuchungsberichte.
  - Kompetenz bei der Formulierung von Ermittlungs- und Präventionsempfehlungen zur Verhinderung zukünftiger Sicherheitsverletzungen
- **Technologische Kompetenz:**
  - Aktuelles Wissen über die neuesten Technologien im Bereich forensischer Informatik.
  - Fähigkeit zur Anpassung an sich entwickelnde Technologien und Methoden.
- **Rechtliche und Ethik-Kenntnisse:**
  - Verständnis der rechtlichen Rahmenbedingungen für forensische Ermittlungen.
  - Einhaltung ethischer Grundsätze bei der Durchführung von Untersuchungen.
- **Kommunikationsfähigkeiten:**
  - Klare und präzise Kommunikation in schriftlicher Form für die Erstellung von Berichten.
  - Effektive mündliche Kommunikation bei der Präsentation von Untersuchungsergebnissen und Empfehlungen.

Ausbildungsprofil: Forensischer Informatik mit Schwerpunkt Cybercrime

- **Hochschulabschluss:**
  - Bachelor- oder Masterabschluss in Informatik, forensischer Informatik, Cybersecurity oder einem verwandten Fachgebiet.

- **Zertifikatsprogramm (zusätzlich):**
  - Zertifizierungen wie Juristische Grundausbildung für Nichtjuristen insbesondere im Bereich Straf- und Prozessrecht.
  - Zertifizierungen wie Certified Information Systems Security Professional, Ethical Hacker oder Certified Computer Forensics Professional.

- **Spezialisierungsausbildung:**
  - Fortbildungen in forensischen Anwendungen wie EnCase, X-Ways und Cellebrite zur Analyse digitaler Beweismittel.
  - Fortbildungen in Programmiersprachen wie Python und Powershell, um neue Analyse- und Ermittlungsmethoden zu entwickeln.

Aufgaben: Ermittlungen im Bereich Cybercrime

- Führung von komplexen Cybercrime-Ermittlungen mit erhöhtem administrativem und zeitlichem Aufwand.
- Operative Leitung von Aktionen und Interventionen in Zusammenarbeit mit der Digitalen Forensik.
- Teilnahme an nationalen und internationalen operativen Meetings, teilweise auch in englischer Sprache.
- Interpretation der forensischen Spurenanalyse und Ableitung der sich daraus ergebenden Ermittlungshandlungen.
- Verfassen von Informations- und Preservation Requests, SIENA- und Interpol-Anfragen, auch in englischer Sprache, sowie nationale Verbreitungen.
- Durchführung von Ermittlungsarbeiten und fachlicher Unterstützung für das gesamte Polizeikorps.
- Spezialisierung in OSINF, Kryptowährungen usw., einschliesslich Wissenstransfer.
- Durchführung von Einvernahmen von Beschuldigten und Auskunftspersonen.

Kompetenzprofil: Ermittlungen im Bereich Cybercrime

- **Cybercrime-Ermittlungen:**
  - Umfassende Erfahrung in der Leitung und Durchführung komplexer Cybercrime-Ermittlungen mit einem tiefen Verständnis für die spezifischen Herausforderungen, einschliesslich erhöhtem administrativem und zeitlichem Aufwand.
- **Operative Führung:**
  - Nachweisliche Fähigkeit zur operativen Leitung von Aktionen und Interventionen im Bereich Cybercrime, insbesondere in enger Zusammenarbeit mit dem Team für Digitale Forensik.
- **Internationale Zusammenarbeit:**
  - Erfolgreiche Teilnahme an nationalen und internationalen operativen Meetings, wobei auch die Fähigkeit besteht, in englischer Sprache zu kommunizieren.
- **Forensische Analyse:**
  - Interpretation von forensischen Spurenanalysen mit dem Ziel, daraus ableitbare Ermittlungshandlungen zu entwickeln.
- **Anfragen und Verbreitungen:**
  - Verfassen von Informations- und Preservation Requests, SIENA- und Interpol-Anfragen, sowohl in Deutsch als auch in Englisch.
  - Nationale Verbreitungen von relevanten Informationen im Zusammenhang mit Cybercrime.
- **Ermittlungsarbeiten und Unterstützung:**
  - Aktive Durchführung von Ermittlungsarbeiten im Bereich Cybercrime sowie Bereitstellung von fachlicher Unterstützung für das gesamte Polizeikorps
- **Spezialisierung und Wissenstransfer:**
  - Spezialisierung in den Bereichen OSINF, Kryptowährungen und ähnlichen Themengebieten.
  - Fähigkeit zum Wissenstransfer durch Schulungen und Informationsaustausch im Team.
- **Einvernahmen:**
  - Durchführung von Einvernahmen von Beschuldigten und Auskunftspersonen gemäss den rechtlichen Vorgaben.

Ausbildungsprofil: Ermittlungen im Bereich Cybercrime

- **Fach-/Hochschulabschluss oder höhere Fachschule:**
  - Bachelor- oder Masterabschluss in Informatik, Cybersecurity, Forensik oder Polizist mit einer Lehre im Bereich Informatik, Elektronik oder einem verwandten Fachgebiet.

- **Spezialisierte Schulungen und Zertifizierungen:**
  - Abschluss relevanter Schulungen und Zertifizierungen im Bereich Cybercrime-Ermittlungen und Digitaler Forensik. Beispiele hierfür könnten Certified Cyber Forensics Professional, Certified Information Systems Security Professional, Ethical Hacker oder ähnliche Zertifikate sein.

- **Spezialisierungsausbildung:**
  - Zusätzliche Schulungen oder Weiterbildungen im Bereich OSINF, Kryptowährungen und anderen spezialisierten Themen, um die erforderliche Expertise für die Spezialisierung zu erlangen.

Daraus folgt:

Die Bearbeitung von Cybercrime erfordert ein Team, bestehend aus wissenschaftlichen Mitarbeitern im Bereich Forensik und Polizisten mit entsprechender Weiterbildung.

Dialog

Fragen?