Eingereichter PRIMA-Beitrag

„Private investigation“ im Bereich der IuK-Kriminalität

Zulässigkeit und Verwertbarkeit der Sachverhaltsaufklärung durch Geschädigte oder Dritte

Jens Gruhl
Staatsanwaltschaft Konstanz
jens.gruhl@stakonstanz.justiz.bwl.de

Zusammenfassung

Um sich vor „ungetreuen“ Mitarbeitern oder Dritten zu schützen, setzen Unternehmen auf präventive Maßnahmen und überwachen die Computerarbeitsplätze. Dabei steht ihr Sicherheitsbedürfnis im Widerspruch zum berechtigten Datenschutzinteresse des Nutzers / Mitarbeiters.

Nach Erkennen des Umstands, Opfer eines Angriffs geworden zu sein, stellt sich für Unternehmen als auch für private Nutzer die Frage, ob eigene Maßnahmen ergriffen oder staatliche Stellen um Ermittlungen ersucht werden sollen. Vermuteter Image- und Vertrauensverlust bei Bekannt werden in der Öffentlichkeit oder fehlendes Vertrauen in die Fach- und Sachkenntnis der Strafverfolgungsbehörden, lassen es teilweise angezeigt erscheinen, private Ermittlungen durchzuführen. Der Wunsch, bei einer späteren Anzeige vollständige Informationen vorlegen zu können, ohne selbst in die Ermittlungen weiter einbezogen zu werden, mag ebenfalls eine Rolle spielen.

Diese privaten Ermittlungen sind neben oder auch an Stelle der staatlichen Maßnahmen nicht verboten, sie können vielmehr bei Berücksichtigung der Belange der Strafverfolgungsbehörden von großem Nutzen sein. Auch wenn – selbstverständlich – die privaten Ermittlungsmaßnahmen im Rahmen des geltenden Rechts erfolgen müssen, sind bspw. Ländergrenzen kein Hindernis. Hier können nichtstaatliche Maßnahmen sogar im zeitlichen Vorteil sein.

Einleitung

Die – tatsächliche (Gruhl in [Welp] S. 52 ff) – und auch subjektiv gespürte Zunahme von computerbasierten Straftaten ([Adamczewski]; [McClure]; [Müller]) führt einerseits zu einem Gefühl der Unsicherheit in der Bevölkerung, andererseits zu dem Ruf nach effizienter (strafrechtlicher) Verfolgung. Mannigfaltige Gründe lassen aber Unternehmen, aber auch Einzelpersonen vor einer frühzeitigen Einschaltung staatlicher Stellen zurückschrecken. Hier stellt sich die Frage, ob präventive Maßnahmen oder – nach einem „incident“ – eigene Ermittlungen die Arbeit der staatlichen Stellen unterstützen oder stören könnten. Die strenge Bindung der staatlichen Stellen an Recht und Gesetz hat zudem zur Folge, dass auch privaten Gegenmaßnahmen oder Ermittlungen Grenzen gesetzt sind. Auch stehen dem Wunsch nach „total information“ die Bestimmungen des Datenschutzes entgegen.

1 Computerkriminalität als Herausforderung

Nach Erkennen des Umstands, Opfer eines Angriffs geworden zu sein, stellt sich für Unternehmen als auch für private Nutzer die Frage, ob eigene Maßnahmen ergriffen werden oder staatliche Stellen um Ermittlungen ersucht werden sollen ([MüGu WiStR] § 42 Rn. 81 ff). Die Erwägungen

- vermuteter Image- und Vertrauensverlust bei Bekannt werden in der Öffentlichkeit ([Geschonneck] 10.4),
- relativ gering ausgeprägtes Interesse an einer Strafverfolgung; zivilrechtliche Ansprüche stehen im Vordergrund,
- Unternehmen ziehen es u. U. vor, eigene Mitarbeiterinnen und Mitarbeiter, die Täter eines entsprechenden Delikts sind, ohne Einschaltung der Strafverfolgungsbehörden selbst zu sanktionieren ([Ernst] Rn. 701 ff),
- fehlendes Vertrauen in die Fach- und Sachkenntnis der Strafverfolgungsbehörden,

lassen es oftmals angezeigt erscheinen, private Ermittlungen durchzuführen. Der Wunsch, bei einer späteren Anzeige vollständige Informationen vorlegen zu können, ohne selbst in die Ermittlungen weiter einbezogen zu werden, mag ebenfalls eine Rolle spielen. Andererseits vermuten Polizei und Staatsanwaltschaft oft nicht zu Unrecht, dass staatliche Maßnahmen nur „Druck“ auf den Täter ausüben sollen, um zu einem gewünschten (zivilrechtlichen) Ergebnis wie Schadenersatzzahlungen o.ä. zu kommen, oder für anstehende (wettbewerbliche) Maßnahmen Beweismittel zu erhalten, die mit eigenen privaten Ermittlungen nicht zu erlangen sind ([Dammann]). Dies kann den Umfang der Ermittlungen der staatlichen Stellen negativ beeinflussen.

2 Präventive Maßnahmen

Verfolgt man Medienberichte ([Borchers]), stellt sich die Frage „Befinden wir uns auf dem besten Weg zu Orwells „Big Brother“?“ allen Ernstes.

Denn um gegen Angriffe gewappnet zu sein, setzen Unternehmen auf präventive Maßnahmen. Nach verschiedenen Erhebungen aus dem Jahre 2001 sollen 27 Prozent aller Computerarbeitsplätze auf der ganzen Welt überwacht werden, auf 27 Millionen PCs soll Spionage-Software laufen, so dass entsprechend viele Unternehmen lückenlose Protokolle von dem Tun ihrer Mitarbeiter – heimlich – aufzeichnen können. Diese Programme registrieren alles, was am oder um den PC herum geschieht: Dateioperationen, Programmstarts, Screenshots, E-Mail-Verkehr, Tastatureingaben und sogar Bildaufnahmen mit Webcams . Beispielsweise überwachen die Programme „surfpatrol“, „STARR“ oder „Spector“ die Nutzung des Computers am Arbeitsplatz oder Zuhause „im Auftrag“ von Personen, die wie der Überwachte Zugang zum Computer haben. Andere Programme wie „Gridpatrol“ überwachen das Internet selbst, um bspw. Verstöße gegen gewerbliche Schutzrechte aufzudecken ([Borchers]; [Ehrmann]). Argument für die Nutzung solcher Software ist sicher auch die an jeden Nutzer von Online-Diensten gerichtete Empfehlung, Schutzmaßnahmen wie Virenscanner oder Firewalls einzusetzen, um Angriffe von außen abzuwehren und so eigene Rechte zu schützen. In Erweiterung dieser Empfehlung raten verschiedene Anbieter, die von ihnen angebotene Überwachungssoftware einzusetzen. Allerdings ist in Deutschland der Einsatz von Überwachungssoftware nur ausnahmsweise und bei Einhaltung bestimmter Regularien erlaubt ([Emmert]). Hinweise wie „Hallo, dieser PC wird überwacht!“, Erklärungen in Lizenzbedingungen oder Formulierungen wie „Mit dem Start dieses PC sind Sie einverstanden, dass alle Tastaturanschläge aufgezeichnet werden.“ genügen jedenfalls nicht ([Borchers]).

Zulässig ist im Arbeitgeber / Arbeitnehmer-Verhältnis nur eine Vereinbarung mit dem Mitarbeiter selbst bzw. der Personalvertretung oder Betriebsrat über Nutzung des Computers oder des Internets. Die Überwachung des Mitarbeiters fällt hierunter nicht. Zulässig ist weiter die Überwachung des unterneh-

menseigenen Netzwerks, um „Einbrüche“ oder Leistungseinbrüche zu erkennen (Reichenbach in [Ernst] Rn. 937 ff).

Zulässig ist schließlich, in einer Betriebsvereinbarung die private Nutzung des Internets im Betrieb und die Speicherung von Daten ([Geschonneck] 4.4.2, 4.4.3) bis hin zum, Verbot privater Nutzung zu regeln. Eine „verdachtsunabhängige“ Kontrolle oder Rasterfahndung ist aber unzulässig [Schoen].

3 Repressive Maßnahmen

Immer wieder wird der Verdacht aufkommen, dass ein Mitarbeiter unter Nutzung firmeneigener Ressourcen eine Straftat begeht oder begangen hat, oder dass das Unternehmen einem Angriff Externer ausgesetzt ist. Es müssen dann Maßnahmen zur Beseitigung eines aktuellen Angriffs, zur Feststellung des Sachverhalts und zur Behebung von Schäden ergriffen werden. Zukünftige Angriffe sollen verhindert und der Täter in irgend einer Form sanktioniert werden.

3.1 Datensammlung

Geschädigten Personen und Unternehmen, aber auch Verbänden steht es im Rahmen der Gesetze grundsätzlich frei, im eigenen Interesse Daten zu sammeln und sie selbst betreffende Vorgänge aufzuklären ([Röscheisen]). Die Pflicht, strafbares Verhalten anderer Personen anzuzeigen, besteht im Bereich der hier angesprochenen IuK-Kriminalität im Allgemeinen nicht ([Haurand/Vahle]; [Maier]). Der „Sammelwut“ und der Verwendung von Daten anderer Personen stehen aber oftmals die Bestimmungen des Datenschutzes entgegen, wie sie im BDSG und den Datenschutzgesetzen der Länder kodiert sind.

Auch das Strafgesetzbuch setzt dem „Forschungsdrang“ Privater Grenzen. Es liegt auf der Hand, dass ein eigener Rechtsbruch nicht mit dem (früheren) Rechtsbruch eines anderen gerechtfertigt werden kann. Notwehr nach § 32 StGB ([T/F StGB] § 32 Rn. 6a)oder das Festnahmerecht des Privatmannes nach § 127 Abs. 1 StPO können allenfalls bei auf frischer Tat betroffenen oder verfolgten Delinquenten rechtfertigend herangezogen werden. Im IuK-Bereich dürfte dies aber in den seltensten Fällen praktisch werden, wenn nicht die Wiederholung der Angriffshandlung unmittelbar zu befürchten ist ([T/F StGB] § 32 Rn. 10). Daneben sind insbesondere die Regelungen des Arbeitsrechts zu beachten und – nicht zuletzt – das Grundrecht auf informationelle Selbstbestimmung.

3.2 Private Ermittlungskräfte

Da Unternehmen mit eigener IuK-Abteilung zwar Fachleute für den Betrieb der IuK-Infrastruktur beschäftigen, aber investigativ tätige Mitarbeiter (Firmenschutz o.ä.) oftmals nicht zur Verfügung stehen, werden für eigene Ermittlungen Mitarbeiter eingesetzt, die hierfür weder juristisch noch kriminalistisch ausgebildet sind. Rein technisches Wissen führt zudem u.U. dazu, dass Beweise statt gesichert unwiederbringlich vernichtet werden ([Meseke]). Hier vermag der Einsatz externer Kräfte von Detekteien oder von auf Sicherheitsfragen spezialisierter Beratungsunternehmen von Nutzen sein ([Jungfer]).

Unternehmen der IT-Industrie setzen dagegen eigene „IT-Ermittler“ ein. Die Business Software Alliance BSA, die die Interessen der Software-Entwickler vertritt, und die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen GVU – um nur die bekanntesten zu nennen – beschäftigen zahlreiche Mitarbeiter, die inzwischen auch online auf die Jagd nach Rechtsverletzern gehen. Internationale Unternehmen wie Microsoft unterhalten eigene Anti-Piraterie-Abteilungen. Durch die Beobachtung der „scene“, durch die Suche (mittels Suchmaschinen) nach Webseiten sowie durch die Teilnahme an Internetauktionen werden zahlreiche Taten aufgedeckt und den Strafverfolgungsbehörden durch Anzeigen bekannt gemacht. Diese privaten Ermittler sind – natürlich – an die Bestimmungen der Rechtshilfe nicht gebunden

und können daher problemlos auch grenzüberschreitend tätig werden (Schorr/Schultis in [Ernst] Rn. 931 ff).

3.3 Beweiserhebung und -verwertung

Die „private investigation“ hat wie die Ermittlungsarbeit der Strafverfolgungsbehörden das Ziel, einen Sachverhalt nachvollziehbar und nachweislich aufzuklären. Die gewonnenen Beweise sollen ggf. in einem gerichtlichen Verfahren verwertet werden, sie müssen „gerichtsfest“ sein. Im Gegensatz zum Beibringungsgrundsatz des Zivilverfahrens, der den Prozessparteien auferlegt, den zur Entscheidung durch das Gericht gestellten Sachverhalt schlüssig vorzutragen und zu beweisen, wird das Ermittlungs- bzw. Strafverfahren vom Grundsatz der Amtsermittlung beherrscht. Es ist Aufgabe der staatlichen Strafverfolgungsbehörden, den Sachverhalt – einschließlich der entlastenden Umstände – vollständig aufzuklären. Hieraus folgt, dass bspw. die Staatsanwaltschaft die Ermittlungen nicht an den Geschädigten oder an ein Privatunternehmen delegieren oder „outsourcen“ kann. Die Strafverfolgungsbehörden sind aber nicht nur bereit, sondern wegen ihres Auftrages zur Sachverhaltsaufklärung auch gezwungen, die vom Geschädigten vorgelegten Beweise zur Kenntnis zu nehmen und zu bewerten ([M-G StPO] § 244 Rn. 11 ff).

Dennoch wird der Geschädigte deshalb prozessual nie „Partei“, auch wenn er bei bestimmten Rechtsverletzungen als Nebenkläger nach § 395 StPO auftreten kann ([Eisenberg] Rn. 1025). Auch im Verhältnis zur Polizei bleibt die Staatsanwaltschaft „Herrin des Verfahrens“, der die abschließende Entscheidung über den Ausgang des Ermittlungsverfahrens zufällt (§§ 152, 151, 170 StPO).

3.3.1 Zeugen und Sachverständige

Bei – wie es in § 170 Abs. 1 StPO festgelegt ist – „genügendem Anlass“ ist Klage zu erheben. Dies ist dann gegeben, wenn der Staatsanwalt nach Sach- und Rechtslage am Ende einer Hauptverhandlung zum Antrag auf Verurteilung gelangen würde ([M-G StPO] § 170 Rn. 2). Bei der Prognose ist danach eine Bewertung der vorhandenen Beweismittel nach den für das Gericht geltenden Maßstäben erforderlich. Die dem Gericht vorzulegenden Beweismittel müssen daher

- rechtskonform erlangt und
- verwertbar

sein („Strengbeweis“: [Eisenberg] Rn. 35). Sie müssen, soweit sie in der Hauptverhandlung verwendet werden sollen, den Anforderungen der oben genannten Beweismittel entsprechen. Diesen Maßstäben müssen folglich auch die Beweismittel entsprechen, die im Rahmen einer „private investigation“ erlangt wurden, wenn sie im Strafverfahren Verwendung finden sollen.

Allerdings sind private Ermittler grundsätzlich nicht an die Regularien der Strafprozessordnung gebunden, die bspw. bei der einer Vernehmung die Teilnahme Dritter (Verteidiger bei Beschuldigten) ermöglichen. Auch eine Belehrung i.S.v. § 136 Abs. 1 StPO müssen private Ermittler nicht geben. Selbst „verbotene Vernehmungsmethoden“ nach § 136a StPO sind Privatpersonen nicht untersagt, soweit sie nicht sonstige Strafgesetze (z.B. Körperverletzung, Freiheitsberaubung, Nötigung, Beleidigung) verletzen ([M-G StPO] § 136a Rn. 3, 31). Solche Vernehmungen dürfen die staatlichen Organe allerdings grundsätzlich nicht ausnutzen ([M-G StPO] § 136a Rn. 3, 4a, 4b). Auch dem früher durchaus üblichen Mithören von Telefonaten durch Dritte hat das Bundesverfassungsgericht in seiner Entscheidung vom 9.10.2002 (1 BvR 805, 1611/98) einen „Riegel vorgeschoben“: „Allein das allgemeine Interesse an einer funktionstüchtigen Straf- und Zivilrechtspflege reicht aber nicht, um im Rahmen der Abwägung stets von einem gleichen oder gar höheren Gewicht ausgehen zu können, als es dem allgemeinen Persönlichkeitsrecht zukommt. Vielmehr müssen weitere Aspekte hinzutreten, die ergeben, dass das Interesse an der

Beweiserhebung trotz der Persönlichkeitsbeeinträchtigung schutzbedürftig ist. Im Strafverfahren kann dies etwa die Aufklärung besonders schwerer Straftaten sein."

Da bei der Erhebung von Beweisen das allgemeine Persönlichkeitsrecht oder das Grundrecht auf informationelle Selbstbestimmung stets beeinträchtigt werden kann (BVerfG NJW 1984, 419), ist bei privaten Ermittlungen letztlich auch darauf zu achten, dass die Rechte des Betroffenen gewahrt bleiben. Das telefonische oder persönliche Gespräch eines privaten Ermittlers, der nicht – auch nicht mittelbar – im Auftrag der Strafverfolgungsbehörden tätig wird, bleibt aber auch nach der oben zitierten Rechtsprechung des Bundesverfassungsgerichts möglich (BGHSt 42, 139). Der private Ermittler kann gegenüber Staatsanwaltschaft und Gericht über den Inhalt des Gesprächs als Zeuge aussagen.

Außer den „klassischen" privaten Ermittlern (Privatdetektiv) kommen auch spezialisierte Fachleute der Computertechnik zum Einsatz, die von den Strafverfolgungsbehörden auch als Sachverständige eingesetzt werden könnten. Soweit diese Fachleute im Auftrag des Geschädigten tätig werden, kommt – wegen der Besorgnis der Befangenheit – eine direkte Beauftragung durch die Justiz nicht in Betracht. Sie stehen aber als fachkundige Zeugen zur Verfügung. Gegen ihre Verwertung im Verfahren im Rahmen der richterlichen Beweiswürdigung, die in vergleichbarer Weise auch der Staatsanwalt vornimmt, bestehen keine Bedenken. Trotz einer – beruflichen – Beziehung zum Geschädigten und einer dadurch bedingten „Gegnerschaft" zum Täter lassen sich die Argumente, die für die Bewertung einer polizeilichen Aussage verwendet werden, in gleicher Weise auf diese berufsmäßigen, persönlich i.d.R. nicht involvierten Zeugen anwenden ([Eisenberg] Rn. 1455).

Neben den genannten Ermittlern beauftragen Geschädigte auch Fachleute, um Sachverhalte festzustellen und Beweise fachmännisch zu sichern. Über diese Maßnahmen werden, um sie nachvollziehbar sowohl dem Auftraggeber als auch der Justiz präsentieren zu können, qualifizierte schriftliche Berichte mit Fotografien, Filmaufzeichnungen u.a. gefertigt ([Eisenberg] Rn. 2005: als „Absichtsurkunde" dem Urkundenbeweis zugänglich; [Grunwald]). Ihre Feststellungen sind zum einen als Zeugenbeweis verwertbar, ihre Berichte über Abläufe technischer Vorgänge können dazu als Gutachten eines Sachverständigen Eingang in das Verfahren finden ([Eisenberg] Rn. 858; [M-G StPO] vor § 72 Rn. 6).

Allerdings ist ihre Bestellung als Sachverständiger nach § 73 Abs. 1, § 161a Abs. 1 S. 2 StPO in der Praxis nicht zu erwarten, da Ablehnung wegen der Besorgnis der Befangenheit durch den beschuldigten bzw. angeklagten Täter zu erwarten sein wird. Der Fachmann wird dennoch als sog. sachverständiger Zeuge gehört werden ([Eisenberg] Rn. 1514 f, 1560 f).

3.3.2 Urkunden und Augenschein

Als Urkunden können nach § 249 StPO alle deutschsprachigen, (menschlich) lesbaren Dokumente verwertet werden. Für Observationsberichte und sonstige Tatsachenberichte einschließlich privater Gutachten gelten §§ 250, 251 StPO. Formale oder prozessuale Besonderheiten bestehen hier nicht, auch was ihren Beweiswert oder die richterliche Würdigung anbelangt.

Augescheinsgegenstände als sachliche Beweismittel sind z.B. Lichtbilder und Videoaufnahmen wie auch Experimente und Rekonstruktionen, die im Verfahren vor Gericht in Augenschein genommen werden. Die Dokumentation anderweitig vorgenommener Versuche oder Feststellungen ist durch andere Beweismittel, i.d.R. durch Zeugen, in das Verfahren einzuführen.

Von besonderer Bedeutung ist verständlicher Weise die Vornahme von Versuchen „lege artis" und die vollständige Erfassung der für die Beurteilung erforderlichen Informationen durch private Ermittler ([Geschonneck] 4.4.4 – 4.4.6).

Fazit

Private Ermittlungen sind neben oder auch an Stelle der staatlichen Maßnahmen nicht verboten, sie können vielmehr bei Berücksichtigung der Belange der Strafverfolgungsbehörden von großem Nutzen sein. Auch wenn – selbstverständlich – die privaten Ermittlungsmaßnahmen im Rahmen des geltenden Rechts erfolgen müssen, sind bspw. Ländergrenzen kein Hindernis. Hier kann die nichtstaatliche „private investigation“ sogar im zeitlichen Vorteil sein.

Auch die Furcht, private Ermittlungsmaßnahmen seien zwar nicht umsonst (d.h. kostenlos), aber folgenlos, ist grundsätzlich nicht angebracht. Gerade im Bereich des gewerblichen Rechtsschutzes besteht eine lange Zusammenarbeit mit privaten Institutionen, was nicht nur daran liegen dürfte, dass z.T. pensionierte Polizeibeamte dort tätig werden. Das Einhalten rechtlicher und technischer Standards bei der Beweiserhebung und Präsentation, verbunden mit einer Offenheit, was die – berechtigte – Verfolgung eigener Interessen und Rechte betrifft, wird den Nutzen privater Ermittlungsmaßnahmen gerade im IuK-Umfeld für alle Beteiligte erkennen lassen.

Literatur

Adamczewski, Piratensport - Spiele-Crackergruppen und Ermittlerarbeit: Einblicke in zwei feindliche Welten, c´t 20/2002, 106 [Adamczewski]

Borchers, Big Brother am Arbeitsplatz - Programme, die Sie unbemerkt ausspionieren, c’t 15/2002, 132 [Borchers]

Dammann, Computerkriminalität aus Sicht von Ermittlungsbehörden, 6. DFN-CERT Workshop "Sicherheit in vernetzten Systemen" [Dammann]

Ehrmann, Erwischt! - Videoüberwachung per Webcam, c´t 2/2003, 124 [Ehrmann]

Eisenberg, Beweisrecht der StPO, 4. Aufl. 2002 [Eisenberg]

Emmert, Strafbare Sicherheits-Tools? KES 2002/2, 6 [Emmert]

Ernst, Hacker, Cracker & Computerviren, 2004 [Ernst]

Geschonneck, Computer Forensik. Systemeinbrüche erkennen, ermitteln, aufklären, 2004 [Geschonneck]

Grunwald, Ausgrabungen - Beweissicherung bei Computerdelikten, iX 10/2002, 100 [Grunwald]

Haurand/Vahle, Eigenmächtige Durchsetzung von Rechten - Unter welchen Umständen darf der Einzelne zur Selbsthilfe greifen?, DVP 2002, 223 [Haurand/Vahle]

Jaeger, Computerkriminalität, 2. Aufl. 2002 [Jaeger]

Jungfer, Strafverteidiger und Detektiv, StV 1989, 495 [Jungfer]

Maier, Verbrechensaufklärung durch Privatdetektive -- Oder - Sind Ermittlungen im Strafverfahren eine rein hoheitliche Aufgabe?, Kriminalistik 2001, 670 [Maier]

McClure/Scambray/Kurtz, Das Anti-Hacker-Buch, 4. Aufl 2003 [McClure]

Meseke, Ermittlungen im Internet - Positionen und Dissonanzen, Kriminalistik 2000, 245 [Meseke]

Meyer-Goßner, Strafprozessordnung, 47. Aufl. 2004 [M-G StPO]

Müller, Kinderspiel - So spionieren Hacker Ihre geheimen Daten aus, Internet Professionell 01/2002, 72 [Müller]

Müller-Gugenberger/Bieneck (Hg.), Wirtschaftsstrafrecht - Handbuch des Wirtschaftsstraf- und -ordnungswidrigkeitenrechts, 3. Aufl. 2000 [MüGu WiStR]

Röscheisen, Spurensuche. Von IP-Adressen zu Ortsinformationen, iX 8/2002, 90 [Röscheisen]

Schoen, Rechtliche Rahmenbedingungen zur Analyse von Log-Files, DuD 2/2005, 84 [Schoen]

Tröndle/Fischer, Strafgesetzbuch, 52. Aufl. 2004 (T/F StGB]

Welp, Kriminalität@net, 2003 [Welp]