Transkript Podcastfolge: Hacks für mehr Cybersicherheit

Ein Beitrag von Klaus Palenberg, Johanna Voget, Nicolas John und Ole-Christian Tech, 5. Juli 2023

Beschreibung:

In dieser Folge behandeln die wissenschaftlichen Mitarbeiter:innen Johanna Voget und Klaus Palenberg das Thema White Hat Hacking. Die rechtliche Zulässigkeit solcher simulierter Cyberangriffe, die dazu dienen Sicherheitslücken im eigenen System ausfindig zu machen und zu beseitigen, wirft einige Fragen und Probleme auf. Diese werden eingehend untersucht und ausführlich besprochen.

Ein Beitrag zum Thema findet sich ebenfalls in der Juliausgabe des DFN-Infobrief Recht.

Transkript

00:00:06 Tech

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN.

00:00:15 Palenberg

Hallo und herzlich Willkommen zu einer neuen Ausgabe von „Weggeforscht“. Heute am Mikrofon sind für Sie meine Kollegin Johanna Voget und ich, Klaus Palenberg.

00:00:23 Voget

Ja, auch von mir ein herzliches Willkommen.

00:00:26 Palenberg

Die Angst Cyberangriffen ist ein ständiger Begleiter sowohl von privaten Unternehmen als inzwischen auch von staatlichen Hochschulen und Forschungseinrichtungen geworden. Aus diesem Grund behandeln wir heute das sogenannte White Hat Hacking. Darunter, simulierte Cyberangriffe zu verstehen, die darauf ausgerichtet sind, Sicherheitslücken im eigenen System ausfindig zu machen und zu beseitigen. Die rechtliche Zulässigkeit solcher Angriffe ist aber problematisch und soll von uns heute näher beleuchtet werden. Doch zuerst, was gibt es Neues?

00:00:53 John

Bildaufnahmen einer Drohne fallen nicht unter die Panoramafreiheit. Das OLG Hamm hat in einer Streitigkeit zwischen einem Verlag und einer Verwertungsgesellschaft entschieden, das Bildaufnahmen einer Drohne nicht von der sogenannten Panoramafreiheit gedeckt sind. Diese gestattet unter anderem die gewerbliche Nutzung von Fotografien von Werken, die sich an öffentlichen Straßen oder Plätzen befinden. Jedoch müssen diese Aufnahmen aus der Perspektive der Öffentlichen Straße oder Plätze aufgenommen sein, um von der Panoramafreiheit gedeckt zu sein. Eine Aufnahme mit einer Drohne wird laut den Richtern des OLG Hamm von der Panoramafreiheit nicht erfasst. Eine endgültige Entscheidung des BGH ist zu erwarten.

BGH entscheidet zum Recht auf Vergessen: Der BGH entschied nun in Orientierung an einem vorhergegangenen Urteil des EUGH, dass Menschen, die ihr Recht auf Löschung aus der DSGVO bezüglich eines Suchmaschinen Eintrags erreichen wollen, hinreichende Nachweise dafür vorlegen müssen. Diese müssen offenkundig zeigen, dass die enthaltenen Informationen unrichtig seien. Die Betreiber der Suchmaschine müssen für die Erlangung dieser Nachweise selbst nicht tätig werden. Soweit die Informationen unrichtig sind, sind diese aus den Suchergebnissen aber zu löschen.

00:01:59 Palenberg

Zuletzt sind Hochschulen und andere öffentliche Stellen immer häufiger ins Visier von Cyberkriminellen geraten. Oft wird dabei sogenannte Rand-Software eingesetzt, die den Betrieb des Computers unmöglich macht oder die gespeicherten Daten verschlüsselt. Dann wird die Zahlung eines Geldbetrages verlangt, damit diese Beschränkungen aufgehoben werden. Johanna, du hast dich näher mit dem Thema White Hat Hacking auseinandergesetzt. Bestehen denn zunächst erstmal rechtliche Verpflichtungen dazu, sich gegen solche Angriffe überhaupt zu schützen?

00:02:27 Voget

Ja, aus der DSGVO folgt zunächst grundsätzlich die Pflicht zur Nutzung technischer und organisatorischer Maßnahmen zur Datensicherheit. Dasselbe gilt auch nach dem Telekommunikations-Telemedien- Datenschutz- Gesetz, kurz TTDSG, auch für die Sicherung von Telemedienangeboten.

00:02:43 Palenberg

Wir könnten solche Maßnahmen beispielsweise aussehen?

00:02:46 Voget

Ja, da gibt es verschiedene Möglichkeiten. Denkbar sind dabei exemplarisch sogenannte Code Reviews, Grundschutz oder ISO Zertifizierungen und eine Alternative dazu wäre eben, das sogenannte White Hat Hacking, mit dem wir uns heute beschäftigen wollen, was ja dazu geeignet ist, Sicherheitslücken im System ausfindig zu machen und diese dann gezielt zu schließen. Also auch das ist natürlich eine Maßnahme, die letzten Endes der Datensicherheit dient.

00:03:10 Palenberg

Was unterscheidet denn diese Art von Hacking von anderen Arten des Hackings? Und warum wird sie White Hat Hacking genannt?

00:03:16 Voget

Ja, das White Hacking zielt eben gerade nicht darauf ab, was man sonst beim Hacking immer so direkt im Hinterkopf hat, dem Betreiber zu schaden, also dem Inhaber des IT Systems, sondern lediglich die Schwachpunkte der IT Infrastruktur zu identifizieren. Die Hacker handeln also mit guten Absichten, tragen also, bildlich gesprochen, eben weiße Hüte. Im Rahmen von sogenannten Penetration-Tests kann sehr effizient erkannt werden, wo in der Sicherheitsarchitektur noch nachgebessert werden muss. Diese Tests werden vom Bundesamt für Sicherheit in der Informationstechnik, kurz BSI, bei IT Systemen mit erhöhtem Schutzbedarf sogar grundsätzlich auch empfohlen. Teilweise werden dann Externe, also selbstständig arbeitende White Hat Hacker von Unternehmen und Systembetreibern, also den privaten oder staatlichen Akteuren, beauftragt und einige Unternehmen, für die bietet es sich eben auch an, die eigene IT -Abteilung einzuschalten und durch diese solche Tests vornehmen zu lassen.

00:04:14 Palenberg

Jetzt wollen wir uns heute mal mit der Rechtslage zu diesem Thema beschäftigen. Gibt es denn rechtssichere Möglichkeiten für die Hacker, solche Hacks überhaupt vorzunehmen?

00:04:22 Voget

Ja, genau das ist heute unser Casus Knacksus. Das ist nämlich leider nicht ganz unproblematisch. Zunächst existiert ein tatsächlich sogar strafrechtliches Risiko, was ja bei den meisten die Alarmglocken direkt sehr schnellen lässt. Nach 202a StGB macht sich strafbar, wer sich unbefugten Zugang zu nicht für ihn selbst bestimmten Daten unter Überwindung einer Zugangssicherung verschafft. Also in der Praxis prüft man dann eben erstmal zunächst, ob eine solche Zugangssicherung überhaupt vorliegt und praktisch können solche zum Beispiel in Passwörtern oder Lese- und Schreibberechtigungen, also die normalen Zugangshindernisse, die man sich auch so drunter vorstellen kann, bestehen. Und dann muss der Täter eben auch unbefugt handeln, also er muss unbefugt diese Sicherungen überwinden. Wenn aber ein Einverständnis des Verfügungsbefugten über diese Daten vorliegt, dann entfällt auch die Tatbestandsmäßigkeit. Also sobald jemand sagt, du darfst auf diese Daten zugreifen, dann ist es natürlich nicht mehr unbefugt. Hier liegt dann also eigentlich auch unser Schwerpunkt, wo wir uns heute jetzt im strafrechtlichen Sinne darüber unterhalten wollen. Denn der Gesetzgeber hat selbst in der Begründung von Paragraph 202a StGB hervorgehoben, dass gerade das Aufspüren von Sicherheitslücken nicht strafbar sein soll, wenn der Hacker eben damit beauftragt worden.

00:05:35 Palenberg

Ist das klingt erst mal für mich, als wäre dann die Strafbarkeit des White Hat Hackings vom Gesetzgeber nicht gewollt und auch ausgeschlossen.

00:05:45 Voget

Ja, das ging mir zunächst auch so, so allgemein und plakativ gilt es dann aber leider doch nicht. Zunächst gibt es einige Daten, an denen dem Unternehmer selbst, also oder der staatlichen Stelle, also demjenigen, der den White Hat Hacker beauftragt, selbst die Verfügungsbefugnis fehlen soll. Und dann kann man natürlich auch kein Hacker beauftragen, auf diese Daten zuzugreifen, wenn man schon selber gar nicht richtig befugt ist, sich mit diesen Daten näher auseinanderzusetzen. Und darüber hinaus gibt es noch einen ganz besonders kritischen Anwendungsfall im Kontext von internen Penetration-Tests, also internen White Hat Hacking Maßnahmen, in Bezug auf Arbeitnehmer. Wenn nämlich ein Arbeitnehmer gegebenenfalls sogar weisungswidrig private Daten auf seinen Rechnern oder auf dem Server abspeichert, dann kann durch diese Penetration-Tests ein unbefugter Zugriff durch das Unternehmen selbst auf diese Daten des Arbeitnehmers vorliegen. In der Regel wird dann aber wohl ein Einverständnis des Verfügungsbefugten, also des beauftragenden Unternehmens oder der staatlichen Stelle, den Straftatbestand ausschließen, man kann es halt nur leider nicht verallgemeinern.

00:06:47 Palenberg

Bei welchen Daten könnte das denn abstrakt dann der Fall sein, dass die Verfügungsbefugnis des Unternehmers fehlt?

00:06:54 Voget

Hier wird wohl insbesondere Standard Software, die in den zu testen Computersystemen verwendet wird, genannt. Da hat der Gesetzgeber tatsächlich das verbleibende strafrechtliche Risiko wohl auch

erkannt, denn er hat für Mitarbeiter des BSI bereits eine gesetzliche Ermächtigung zur Testung von am Markt angebotenen Standard Software geschaffen, aber eben nicht für private Tester, also die ganz üblichen, gewerblich agierenden White Hat Hacker.

00:07:20 Palenberg

Okay also das ist jetzt das Problem mit dem ersten Straftatbestand. Kommen da vielleicht noch weitere in Betracht?

00:07:27 Voget

Ja, in Betracht käme wohl auch Paragraph 202c StGB, der ganz eng im Zusammenhang mit dem eben genannten 202a steht und darüber hinaus nur bestimmte Vorbereitungshandlungen für dieses Ausspähen von Daten unter Strafe stellt, also zum Beispiel das Entwickeln und Anbieten oder zur Verfügung stellen von Hack Software. Im Ergebnis dürfte das aber dann beim White Hat Hacking nicht vorliegen, also der Tatbestand dürfte wohl nicht erfüllt sein, denn der soll nur solche Programme verbieten, denen die illegale Verwendung immanent ist, also die wirklich auf die Begehung von Straftaten angelegt ist, diese Software, und nicht auf Software, die auch zu legitimen Zwecken genutzt werden kann.

00:08:08 Palenberg

Ja, also da ist ja einiges noch nicht so hundertprozentig klar. Deswegen würde ich festhalten, dass auf jeden Fall ein strafrechtliches Risiko für White Hat Hacker besteht. Bestehen denn auch noch andere Probleme, zum Beispiel datenschutzrechtliche Probleme?

00:08:23 Voget

Ja, definitiv. Das war ja auch eigentlich gar nicht anders zu erwarten. Der Datenschutz macht ja immer Probleme, also jedenfalls dann, wenn personenbezogene Daten betroffen sind. Und in dieser Antwort liegt irgendwie auch gleichzeitig das Problem, denn es lässt sich ja im Vorhinein gar nicht immer sagen, ob personenbezogene Daten betroffen sein werden. Der Hacker soll ja schließlich durch das Hacking, also diese Penetration Tests, erstmal versuchen sich Zugang zu diesem System zu verschaffen und dann weiß man natürlich auch nicht, aber das schafft und ob er dann im Endeffekt auf personenbezogene Daten trifft. Ansonsten wäre der Test ja auch irgendwie sinnlos, wenn man das vorhin sagen könnte. Sofern personenbezogene Daten in irgendeiner Form durch das Hacking dann aber betroffen werden, sag ich jetzt mal so, liegt aber sofort eine Verarbeitung von personenbezogenen Daten vor, unabhängig davon, ob der Hacker die Daten dann irgendwie tatsächlich zur Kenntnis nimmt, also speichert oder ausliest, weil der Artikel 4 Nummer 2 DSGVO sehr weit gefasst ist und jede Form der Bereitstellung von personenbezogenen Daten erfasst. Und darunter fällt auch eben allein schon dieses, ja, irgendwie in irgendeiner Art Zugriff nehmen im Rahmen eines Hacking Angriffs. Zudem ist in diesem Kontext dann noch zu prüfen, ob der Hacker durch die Beauftragung auch Auftragsverarbeiter im Sinne der DSGVO wird. Also hier liegt noch ein weiteres Problem, wenn er nämlich Auftragsverarbeiter wäre, bedürfte er keine eigenen Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten, sondern könnte sich einfach auf die Stützen, die der Auftraggeber selbst heranziehen kann. Ob jetzt der Hacker Auftragsverarbeiter ist oder nicht, ist wieder sehr einzelfallbezogen und hängt dann eigentlich von der vertraglichen Ausgestaltung der Beauftragung ab, also dem Umfang seiner eigenen Verantwortung, wie weisungsgebunden er ist und was er eigentlich genau vornehmen soll im Rahmen dieses beauftragten White Hat Hacking Angriffs.

00:10:10 Palenberg

Wenn wir jetzt also eine Verantwortlichkeit haben, besteht immer die Möglichkeit, dass sich dann der Hacker auf Erlaubnistatbestände nach der DSGVO berufen könnte. Welche kämen da denn in Frage, sofern er jetzt nicht Auftragsverarbeiter allein ist?

00:10:25 Voget

Ja, zunächst denkt man da immer an den wohl besten, sag ich mal, Rechtfertigungstatbestand nach der DSGVO eigentlich, die Einwilligung. Die ist aber natürlich erst mal ein immenser Aufwand. Also wenn man jetzt von jedem möglicherweise betroffenen Arbeitnehmer oder von jedem möglicherweise Betroffenen, von jeder möglichen betroffenen Personen die Einwilligung einholt. Und dann ergibt sich auch das Problem, dass die Einwilligung frei widerruflich ist. Das heißt, sobald dann irgendwie einer sagt, ach nee, doch nicht, dann wäre die rechtliche Zulässigkeit des White Hat Hacking Angriffs auch wieder ins Wanken geraten. Deswegen stellt das grundsätzlich keine taugliche Rechtsgrundlage für die Durchführung von Penetration-Tests dar.

00:11:02 Palenberg

Außerdem ist es ja auch ein bisschen komisch, vorher zu fragen, darf ich dein System zu hacken, wenn ich ja gerade genau das testen soll, ob es denn hackbar ist.

00:11:11 Voget

Ja genau, das stellt auch ein bisschen den Sinn und Zweck des White Hat Hacking Angriffs ein bisschen ad absurdum. Und ja, danach könnte man sich eigentlich nur noch auf das berechtigte Interesse des Verarbeiters stützen als Rechtfertigungstatbestand. Und da ist jetzt zu erwähnen, dass in den Erwägungsgründen zur DSGVO tatsächlich die Sicherheit von IT Systemen auch explizit als berechtigtes Interesse genannt ist. Also da wäre natürlich der White Hat Hacking Angriff dann auch darunter zu subsumieren, man könnte sagen, ja, das ist dann ja wohl ein berechtigtes Interesse, um die IT Sicherheit im Endeffekt zu stärken, aber da ist dann natürlich wieder Einzelfallbetrachtung angesagt, also man müsste wieder immer im Einzelfall klären, immer eine Abwägung der widerstreitenden Interessen vornehmen und dann prüfen, ob denn auch tatsächlich hier das Interesse am Schutz der IT Systeme hier in dem Fall überwiegt.

00:11:59 Palenberg

Ja, also dann verbleibt also auch in dem Bereich noch einiges an Rechtsunsicherheit, so wie ich das verstehe. Jetzt haben wir uns mit konkreten Gesetzen befasst. Gibt es denn auch noch grundrechtliche Positionen, die hier eine Rolle spielen?

00:12:13 Voget

Ja, tatsächlich aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz leitet das Bundesverfassungsgericht ja das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme her. Und dieses wird interessanterweise auch andersrum als staatliche Schutzpflicht verstanden. Eben diese Systeme gegen Angriffe von Dritten zu schützen, um quasi dann halt auch diese Vertraulichkeit und Integrität wiederum zu gewährleisten. Und daraus kann man auch die Pflicht zur Einführung von Ausnahmen im Strafrecht oder Datenschutzrecht, die dann wiederum die die Durchführung von Penetrationstests und White Hat Hacking Angriffen ermöglichen. Da kann man eigentlich auch eine Pflicht des Staates sehen, das auch rechtssicher zu gewährleisten, dass das möglich ist.

00:12:56 Palenberg

Ja, also das klingt auf jeden Fall so. Das hat der Gesetzgeber bislang aber noch nicht gemacht, wie wir festgestellt haben. Gibt es irgendwelche Pläne oder bevorstehende Regelung?

00:13:07 Voget

Ja, also im Koalitionsvertrag ist tatsächlich die Zielsetzung vorhanden. Da ist explizit genannt, dass man durch rechtliche Rahmenbedingungen die legale Durchführung von Identifizierung und Meldung und Schließung von Sicherheitslücken in IT Systemen ermöglichen möchte. Trotz der Empfehlung einer Expertengruppe sind da aber bislang keine konkreten Gesetzgebungsvorhaben bekannt. Auf EU-Ebene ist ja kürzlich die NIS 2 Richtlinie ergangen, über die unsere Kollegen im letzten Podcast ja bereits ausführlich berichtet haben. Aber auch diese schafft jetzt hier keine Lösungen für die jetzt konkret von uns heute thematisierten, ja auch sehr nationalen Strafrecht und, gut, die DSGVO ist auch europaweit harmonisiert, aber die schafft da jetzt keine konkrete Abhilfe, dass man diese Lücken oder diese Probleme im Rahmen des White Hat Hackings konkret jetzt irgendwie schließen würde.

00:13:58 Palenberg

Was bedeutet das denn jetzt für Hochschulen und Forschungseinrichtungen?

00:14:02 Voget

Ja, zunächst einmal, und das ist halt auch das, was viele Unternehmen oder staatliche Einrichtungen beschäftigt, das White Hat Hacking eben nicht risikofrei durchgeführt werden kann, sondern man vorher ganz genau die rechtliche Zulässigkeit prüfen muss und, also insbesondere gilt das, wenn man das halt intern machen möchte und sich jetzt nicht eines externen White Hat Hackers beauftragt, der da vielleicht schon Expertise und langjährige Praxis hat, selbst da ist es nicht komplett sicher immer, aber auch gerade bei internen Maßnahmen gibt es da einfach einiges zu beachten. Man kann nicht einfach so mein System hacken und überprüfen, auch wenn das gute Absichten sind, die dahinter stecken, das geht eben nicht und das hemmt natürlich im Ergebnis auch die Praxis und die IT. Sicherheit insgesamt. Und ja, durch die NIS 2 Richtlinie sollen Hochschulen und Forschungseinrichtungen nun ja auch berechtigt oder gegebenenfalls sogar verpflichtet werden, die Entwicklung, Verbesserung und den Einsatz von IT Sicherheitssystemen zu unterstützen. Und da kann man auch generell eigentlich eine Aufforderung an den nationalen Gesetzgeber darin sehen, endlich rechtssichere Lösungen im Bereich des Strafrechts und Datenschutzrechts zu schaffen, damit Forschungseinrichtungen, Universitäten und auch im Endeffekt private Akteure das auch selber gewährleisten können und auch selber durch White Hat Hacking auch ja eigene Schritte gehen können, um ihre eigenen Systeme zu überprüfen.

00:15:15 Palenberg

Dann sind wir mal gespannt, ob der Gesetzgeber dahingehend tätig wird, was ja eigentlich unerlässlich ist. Aber bis dahin bleibt ja erstmal abzuwarten, wie jetzt die Gerichte und die Behörden, die Aufsichtsbehörden, bis dahin dann mit dem White Hat Hacking umgehen. Ja, die Anwendung der rechtlichen Regelung und damit die rechtliche Zulässigkeit ist dadurch aber natürlich sehr einzelfallbezogen.

00:15:37 Voget

Ja, ganz genau. So kann man das auf jeden Fall gut, kurz und prägnant zusammenfassen und festhalten. Es bleibt spannend beim Thema IT Sicherheit. Und genau, damit wäre es das dann auch mit unserer heutigen Folge. Ich würde sagen, da haben wir wieder einiges weggeforscht.

00:15:50 Palenberg

Ja, vielen Dank, liebe Johanna, für die Erläuterungen und auch Ihnen, liebe Hörerende, vielen Dank fürs Einschalten und Zuhören, bis zum nächsten Mal. Machen Sie es gut.