April 2015

Studie zur Computerkriminalität in Deutschland 2015

Sehr geehrte Damen und Herren,

mit diesem Newsletter möchte ich Ihnen einen Überblick über die Ergebnisse unserer aktuellen Studie zur Computerkriminalität in Deutschland geben. Zum nun dritten Mal veröffentlicht KPMG in Zusammenarbeit mit dem renommierten Sozialforschungsinstitut TNS Emnid die Studie zur Computerkriminalität in Deutschland. Dazu wurden branchenübergreifend 505 Unternehmen unterschiedlichsten Umsatzes zu der Thematik e-Crime befragt.

In den vergangenen zwei Jahren waren 40 Prozent der Befragten Opfer von e-Crime. 2013 traf dies nur auf etwa ein Viertel der Unternehmen zu. Die meist genannten Delikte stellen nach wie vor Computerbetrug sowie das Ausspähen beziehungsweise Abfangen von Daten dar. Jeweils ein Drittel der Opfer von Computerkriminalität war derartigen Angriffen ausgesetzt. Eine bedeutsame Problematik zeichnet sich darin ab, dass die Täter gemäß dem Empfinden der Befragten immer professioneller und häufiger aus dem Ausland vorgehen und daher kaum zurückzuverfolgen sind.

Auf diese sowie weitere Erkenntnisse möchte ich in diesem Newsletter weiter eingehen.

Mit besten Grüßen

Alexander Geschonneck

Alexander Geschonneck
Partner,
Leiter Forensic
KPMG, Forensic Berlin
T +49 30 2068-1520
ageschonneck@kpmg.de

Die Themen der aktuellen Ausgabe

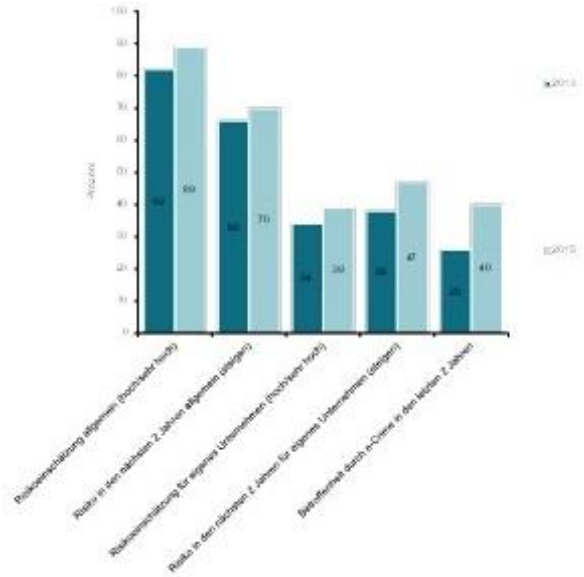
AKTUELLE LINKS

www.kpmg.de/forensic

FOLGEN SIE KPMG

Zwei von fünf Unternehmen betroffen

In den vergangenen zwei Jahren waren 40 Prozent der befragten Unternehmen von e-Crime betroffen. Gegenüber 2013 handelt es sich hierbei um einen Anstieg um 14 Prozentpunkte. Diese Tatsache belegt, dass Unternehmen sich früher oder später mit an Sicherheit grenzender Wahrscheinlichkeit mit Computerkriminalität auseinandersetzen müssen. Selbst die beste Prävention kann dieses Risiko nicht vollständig ausschließen. Es gibt dabei nicht „das eine typische“ e-Crime-Delikt. Allerdings stellt, mit einer Betroffenheitsrate von 37 Prozent, Computerbetrug die meistgenannte Deliktsart dar.



Quelle: KPMG, 2015

Risiko liegt bei den anderen

Nach wie vor zeigt sich, dass Unternehmen dazu neigen, das von e-Crime ausgehende Risiko nicht mit sich selbst, sondern anderen Unternehmen zu assoziieren. So fällt die Risikoeinschätzung für deutsche Unternehmen im Allgemeinen (89 Prozent hohes/sehr hohes Risiko) um 50 Prozentpunkte höher aus als für das eigene Unternehmen (39 Prozent). Dieses Phänomen der Risikoverdrängung trifft dabei nicht nur speziell auf e-Crime, sondern auch auf Wirtschaftskriminalität im Allgemeinen zu.

Risikowahrnehmung und (angegebene) Betroffenheit stimmen nicht überein

Vergleichbar zur Wirtschaftskriminalitätsstudie 2014 besteht eine zum Teil große Diskrepanz zwischen der Risikowahrnehmung und der tatsächlichen Betroffenheit hinsichtlich einzelner Deliktsarten.

Diese Differenz tritt bei den Deliktsarten Datendiebstahl, der Verletzung von Geschäfts- und Betriebsgeheimnissen sowie der Verletzung von Urheberrechten besonders deutlich zu Tage. Keines dieser Delikte verzeichnet eine Betroffenheit von über 15 Prozent. Gleichzeitig

empfinden jedoch mindestens 75 Prozent der Befragten das Risiko, Opfer speziell einer dieser Deliktsarten zu werden, als hoch bzw. sehr hoch.

Dafür können zwei mögliche Ursachen festgestellt werden:

Einerseits handelt es sich bei den oben genannten Delikten um solche, die typischerweise im Fokus der Medien stehen und somit eine gesteigerte Aufmerksamkeit erregen. Daher sind sie möglicherweise im Risikobewusstsein der Befragten präsenter als andere Deliktsarten.

Andererseits gilt gerade für Datendelikte, dass Unternehmen ihre tatsächliche Betroffenheit vielfach nicht korrekt angeben können. Dies liegt zum einen daran, dass es betroffenen Unternehmen vielfach an Überblick und Kontrolle über die komplexen technischen Systeme und Prozesse mangelt, die derartigen Angriffen ausgesetzt sind.

Zudem fehlen den Befragten vielfach geeignete Entdeckungsmechanismen, die diese speziellen Angriffe effektiv erkennen können. Schließlich bedeutet Datendiebstahl eben nicht, dass Daten tatsächlich verschwinden wie materielle Gegenstände. Vielmehr werden sie oftmals unzulässigerweise kopiert und dann andernorts verwendet, was kaum – wenn überhaupt – auffällt. Daher dürfte hinsichtlich datenbezogener Delikte die tatsächliche Dunkelziffer höher ausfallen als die Unternehmen es angeben.

Durch e-Crime verursachter Gesamtschaden deutlich gestiegen

Angesichts der gestiegenen Betroffenheit ist auch der durch e-Crime entstandene Gesamtschaden deutlich angewachsen. Die deutsche Wirtschaft verzeichnete den Ergebnissen der Studie zufolge in den vergangenen zwei Jahren eine Gesamtschadenssumme von 54 Milliarden Euro. Im Vergleich dazu verursachte die e-Crime übergeordnete Wirtschaftskriminalität Gesamtschäden von über 80 Milliarden Euro. Das unterstreicht das immense Gefahrenpotenzial, das von Computerkriminalität ausgeht.

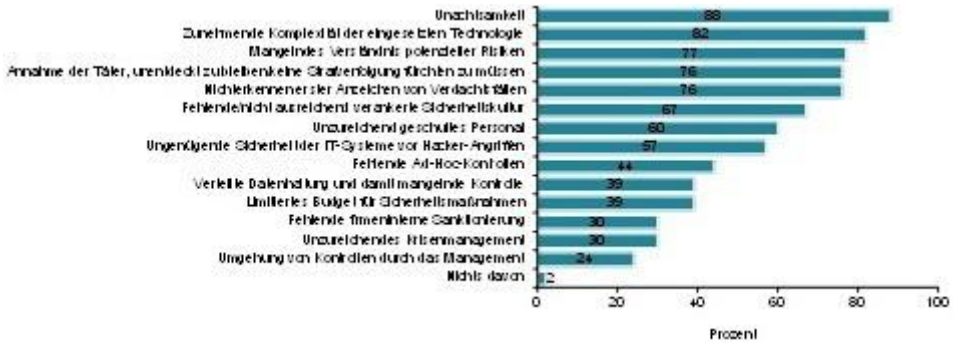
Die durchschnittlichen Kosten eines einzelnen Vorfalls betragen über alle Deliktsarten hinweg 371.000 Euro. In Einzelfällen fallen Summen von über 1.000.000 Euro an. Gegenüber der Vorgängerstudie sind die durchschnittlichen Ermittlungs- und Folgekosten von 100.000 auf 68.000 Euro gesunken. Sie machen damit nur noch einen Anteil von 18 Prozent des Gesamtschadens aus. Dieser setzt sich zusätzlich zu Ermittlungs- und Folgekosten aus Bußgeldern, Geldstrafen oder eventuellen Gewinnabschöpfungen zusammen. Immaterielle Schäden wie Reputationsschäden oder der Verlust an Marktmacht werden in diesem Begriff nicht erfasst.

Die gesunkenen Ermittlungs- und Folgekosten sind möglicherweise damit zu erklären, dass Unternehmen gezielter und somit kosteneffizienter auf Vorfälle reagieren. Inzwischen wird vielfach eine risikoorientierte Vorfallsklassifikation vorgenommen. So können entsprechende Maßnahmen eingeleitet oder gegebenenfalls unterlassen werden, falls das Kosten-Nutzen-Verhältnis nicht stimmig ist.

Mensch bleibt potenziell größter Risikofaktor für e-Crime

In Einklang mit sowohl der Vorgänger- als auch der Studie zur Wirtschaftskriminalität bleibt der Faktor „Mensch“ für die Begehung von e-Crime von größter Bedeutung. 88 Prozent benennen Unachtsamkeit als besonders begünstigenden Faktor für e-Crime. Weitere 77 Prozent führen in dieser Hinsicht ein mangelndes Risikoverständnis der Mitarbeiter an. Beide Faktoren können im Rahmen einer sorgsameren Sensibilisierung und Schulung der Mitarbeiter eingedämmt werden. Die im Bereich der Schulungs- und

Sensibilisierungsmaßnahmen empfundenen Verbesserungen reichen offenbar noch nicht aus, um diese Problematik angemessen zu adressieren.



Quelle: KPMG, 2015

Weitere häufig genannte Faktoren betreffen die zunehmende Komplexität der eingesetzten Technologie (82 Prozent) sowie die damit verbundenen Schwierigkeiten bei der Erkennung erster Anzeichen von Verdachtsfällen (76 Prozent). Diese Problematiken dürften Unternehmen auch in den kommenden Jahren beschäftigen, da man sich dem technologischen Fortschritt und Wandel nicht wird entziehen können.

Abschließend schätzen etwa drei Viertel der Befragten, dass die abschreckende Wirkung von Sanktionen auf Täter ausbleibt. Vielfach gehen sie davon aus, keine Konsequenzen spüren zu müssen. Folglich gestaltet sich die Begehung eines e-Crime-Delikts umso attraktiver.

Professionalisierung und Internationalisierung der Täter

Tatsächlich scheinen die Befragten vermehrt Schwierigkeiten bei der Verfolgung der Täter zu empfinden. In knapp einem Viertel der Fälle blieben Sanktionen aus und somit verfällt auch die abschreckende Wirkung ebenjener.

Ursache ist vor allem die Weiterentwicklung des typischen Täters von e-Crime. Hier lässt sich laut Befragten eine eindeutige Tendenz zur Professionalisierung und Internationalisierung erkennen. So empfinden 94 Prozent der Studienteilnehmer, dass sich hinter den Tätern immer häufiger professionell organisierte Gruppen verbergen. Knapp zwei Drittel der Befragten halten daher die Organisierte Kriminalität für die potenziell gefährlichste Personengruppe hinsichtlich von e-Crime. Hinzu kommt, dass Angreifer vermehrt aus dem Ausland tätig werden (84 Prozent der Befragten nehmen dies so wahr).

In Verbindung mit den immer komplexeren Angriffsmustern und den sonstigen Herausforderungen neuartiger Technologien sind potenzielle Täter teilweise lediglich unter größten Schwierigkeiten zurückverfolgbar, wenn überhaupt. Das äußert sich auch in der Sanktionspraxis.

Sofern die Täter bestraft werden, handelt es sich dabei zumeist um strafrechtliche Konsequenzen. Insbesondere Finanzdienstleister und Handel vertrauen verstärkt auf diesen Sanktionstypus. Die größten Schwierigkeiten bei der Verfolgung haben sonstige Dienstleister. In dieser Branche kam es in über einem Drittel der Vorfälle nicht zu Konsequenzen.

Selbstbewusstsein bröckelt – Investitionsbereitschaft steigt

Angesichts der genannten Problematik nehmen Unternehmen vermehrt Versäumnisse im Umgang mit e-Crime wahr. So gaben 2013 noch 99 Prozent an, dass es solche nicht gegeben hätte; 2015 sind dies immerhin nur noch 75 Prozent.

Schwierigkeiten werden dabei vor allem im Incident Management gesehen. So zählen eine unklare Informationslage, unklare Verantwortlichkeiten sowie die Implementierung und tatsächliche Umsetzung von Sofortmaßnahmen zu den meistgenannten Schwächen.

Insofern ist es erfreulich, dass Unternehmen verstärkt in die Bekämpfung von e-Crime investieren wollen und dabei vor allem Prävention und Detektion ins Auge fassen. Ein solcher präventiver Ansatz minimiert die anfallenden Kosten schon in ihrer Entstehung und ist reaktionsbedingten Investitionen vorzuziehen. Diese erzielen bei gleichen oder sogar höheren Kosten nicht denselben Effekt. Daher entspricht es dem Grundsatz des ökonomischen Prinzips präventiv und detektiv zu investieren, um die Entstehung weiterer Kosten bestmöglich zu verhindern. Durchschnittlich will man in den kommenden zwei Jahren 156.000 Euro investieren (bereits betroffene Unternehmen sogar 250.000 Euro).

Einen vollständigen Überblick über die Studienergebnisse erhalten Sie hier.

Studie „Computerkriminalität in Deutschland 2015“

Bei weiterführenden Fragen zu diesem Thema stehen Ihnen unsere Spezialisten gerne zur Verfügung.

KPMG AG Wirtschaftsprüfungsgesellschaft
Sitz/Registergericht: Berlin/AG Charlottenburg, HRB 106191 B
Vorstand: WP StB Klaus Becker (Sprecher des Vorstandes), WP StB Michael Krall (Stellv. Sprecher), WP CPA Karl Braun, StB Frank W. Grube, WP StB Ingmar Rega

Generalbevollmächtigter: Christian Rast

Aufsichtsratsvorsitzender: WP Ulrich Maas