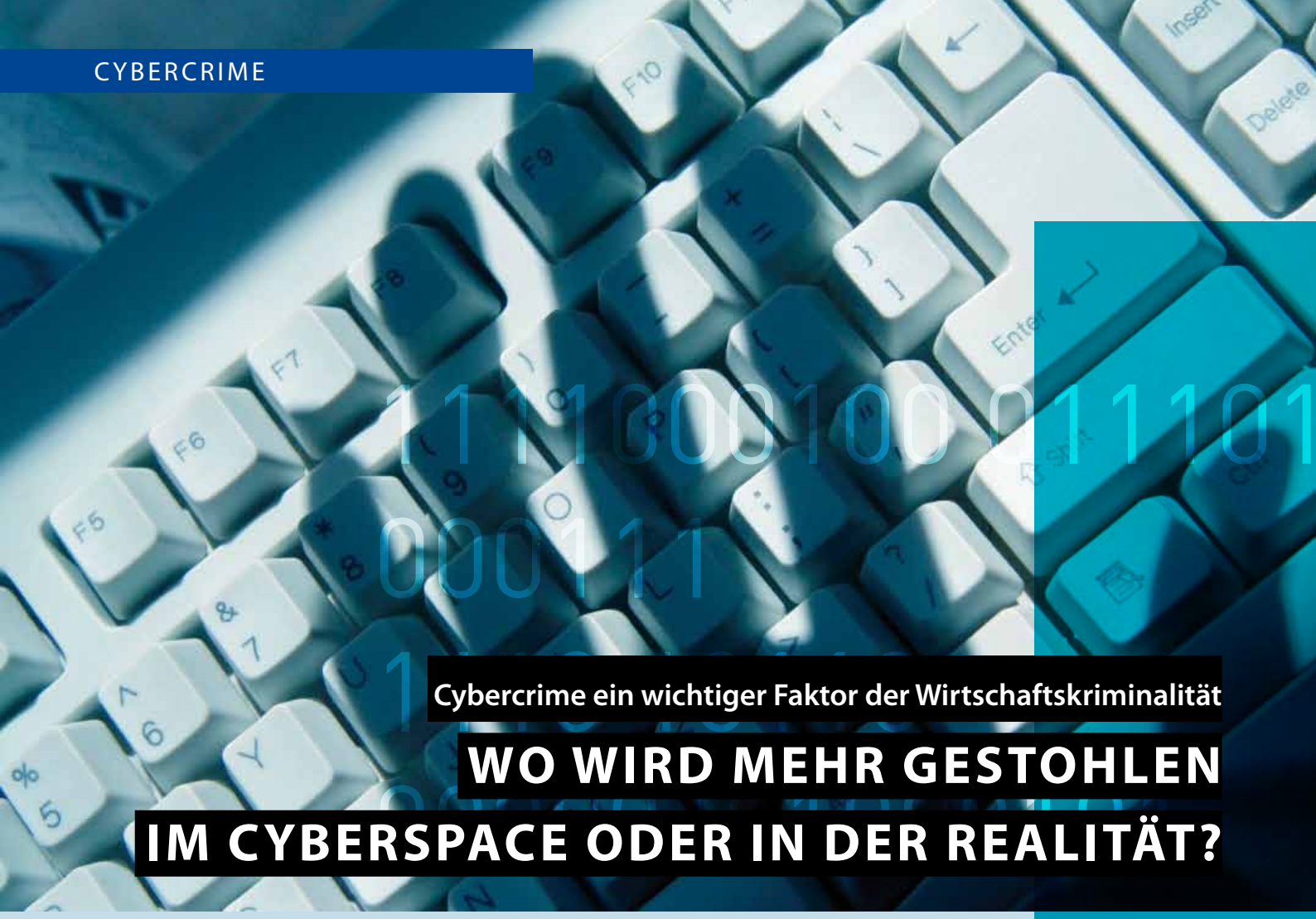


Cybercrime ein wichtiger Faktor der Wirtschaftskriminalität

WO WIRD MEHR GESTOHLEN IM CYBERSPACE ODER IN DER REALITÄT?

Hacker stehlen 1,5 Millionen Kreditkarten-Nummern … geschehen in den USA in den letzten Tagen. Die Angst in den Unternehmen ist gross, alle fürchten sich vor Hacker-Attacken, die ganze Betriebe innert Sekunden lahmlegen können, und gezielte Wirtschaftsspionage über die nicht wirklich sicheren Datensafes. Leider ist diese Befürchtung richtig! Cybercrime entwickelt sich rasant und in ganz diversifizierten Richtungen, von einfachen Spam-Attacken bis hin zu mafiösorganisierter Erpressung findet sich alles, was das kriminell begabte menschliche Hirn sich ausdenken kann.

| von Connie de Neef

Aber Cybercrime ist nur ein Teil der Bedrohung, nach wie vor ist die einfache, innerhalb des Unternehmens verursachte Vermögensveruntreuung immer noch das erfolgreichste und häufigste Wirtschaftsdelikt.

Seit einigen Jahren befragt die PWC (PricewaterhouseCoopers) Beratungs- und Prüfungsgesellschaft weltweit Unternehmen unterschiedlichster Grösse und aus unterschiedlichen Branchen zum Thema Wirtschaftskriminalität. Diese Befragungsergebnisse sind erstaunlich und widerspiegeln einen bedenklichen Sicherheitszustand, die Situation in der Schweiz unterscheidet sich dabei nur zum Teil von der globalen Beurteilung. Die Ergebnisse der Befragung sind öffentlich zugänglich und können auf www.pwc.ch unter Studien eingesehen werden.

Rund 18 % der von PWC befragten Schweizer Unternehmen stellten in den letzten zwölf Monaten einen Fall von Wirtschaftskriminalität in ihrem Unternehmen fest, das ist immerhin fast ein Fünftel aller befragten Unternehmen. Wenn man dazu bedenkt, dass ein grosser Anteil an Wirtschaftskriminalität in den Unternehmen nicht erkannt und auch nicht publik gemacht wird, dann wird klar, dass die Dunkelziffer viel höher liegt, als die PWC-Befragung offenbart. Auch im internationalen Vergleich liegt die Schweiz mit 18 % weit unten dem globalen Mittel von 34 %.

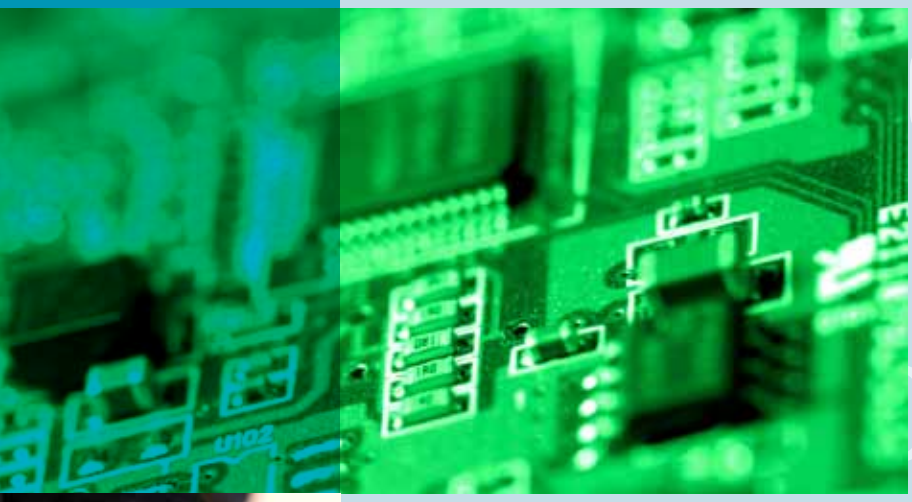
Vermögensveruntreuung versus Cybercrime

80 % aller registrierten Wirtschaftsdelikte waren klassische Vermögensveruntreuungsdelikte (ist von 2009

▶▶

bis 2011 von 64 % auf 80 % gestiegen!). Kriminaldelikte aus der Sparte Cybercrime wurden mit 20 % benannt, gefolgt von Wirtschaftsspionage und Geldwäscherei.

20 % sind Grund genug sich einmal genauer mit der Cybercrime-Bedrohung auseinander zu setzen. Als Cybercrime definierte PWC bei seiner Umfrage Delikte, welche mit Hilfe und Unterstützung eines Computers und/oder dem Internet begangen wurden. Typische Cybercrime-Delikte sind Virus-Attacken, illegaler Download von Daten, Pishing und Pharming und Diebstahl von persönlichen Informationen.



Während bei klassischen Vermögensveruntreuungsdelikten der Verursacher meist innerhalb des Unternehmens zu suchen ist, ist das bei Cybercrime-Attacken plötzlich ganz anders; da mischen und kombinieren sich externe und interne Bedrohungsszenarien und werden dadurch unberechenbar und auch zu einem grossen Stück unkalkulierbar.

Von den befragten Unternehmen wurde aber nicht nur der mögliche Verlust von Daten bei einer Cybercrime-Attacke als gravierend bewertet, sondern auch durch Cybercrime-Attacken entstandene Rufschädigungen und Imageverluste, Diebstahl von geistigem Eigentum, Finanzverlust und als Folge davon verminderte Sharholdervalue. In den kommenden Monaten erwartet die Schweizer Wirtschaft zudem einen erheblichen Anstieg an Cybercrime-Delikten.

Täterprofil? Mitarbeiter oder Kunden?

In der Bedrohungsbeurteilung zeichnet die Schweiz ein anderes Bild als die globale Beurteilung, so sind die Schweizer Unternehmungen der Überzeugung, dass nur 40 % aller Wirtschaftsdelikte von Mitarbeitern begangen wurden, wogegen 52 % aller Delikte von aussen stammen. International präsentieren sich diese Resultate genau umgekehrt; 56 % wurden von Mitarbeitern begangen, 40 % von externen.

Im Vergleich zur Befragung aus dem Jahr 2009 hat sich aber die Qualität der internen Bedrohung verändert. Wo früher das Kader und das Mittelmanagement im Betrug involviert war, werden jetzt neu einfache Mitarbeiter als Verursacher gesehen (2011 = 70 %, 2009 = 30 %) (Mittleres Management 2011 = 10 %, 2009 = 50 %; Kader 2011 und 2009 = 20 %). 50 % aller aufgedeckten Mitarbeitertäter waren zwischen 41 und 50 Jahre alt, 60 % der internen Täter waren bis zur Tatzeit 3 bis 5 Jahre im Unternehmen engagiert.

Die Aussenbedrohung präsentiert sich in der Beurteilung durch die Unternehmen wie folgt: Kunden machen 54 % aller Betrugsfälle aus, andere 15 %, Lieferanten 8 %, Verkäufer 8 % und wir wissen nicht wer 15 %.

Wie schützen sich die Firmen gegen Cyberkriminalität?

Das Verheerende am Cybercrime ist, dass es dafür keinen wirklichen Schutz gibt. Denn einerseits wissen die Unternehmen gar nicht genau, welche Abteilung sie nun mit den meisten Schutzmechanismen ausrüsten sollen, die IT oder die Finanzabteilung oder doch die Forschung und Entwicklung?

Im Zeitalter der schnellen und stetigen Kommunikation sind alle Bereiche miteinander vernetzt und dadurch vergrössert sich die Angriffsfläche enorm.

Weil in den meisten Unternehmen die Zuständigkeit und Verantwortungsfrage i.S. Cybercrime-Schutz nicht geklärt sind, werden Aufgaben oft hin und her geschoben statt gelöst.

Hinzu kommt, dass beinahe jeder Mitarbeiter nicht nur im Unternehmensnetz arbeitet, sondern sich gleichzeitig auch auf Socialmedia-Plattformen bewegt und/oder als neue Arbeitsweise sich ausserhalb der Firma übers Internet Zugang zu den Firmendaten beschafft. Das Gros der Mitarbeiter ist sich bei all den Aktivitäten im Internet der Thematik Sicherheit nicht wirklich bewusst ist.

Kein Wunder also, dass sich kriminelle Elemente den löchrigen Sicherheitsschutz gerne und phantasievoll zu Nutze machen.

Wie wird Cybercrime bekämpft?

Auch die Verfolgung von Cybercrime-Delikten ist nicht einfach. So kämpfte z.B. die Bundesanwaltschaft mit Zuständigkeitsfragen, als sie gegen Pishing-Mafia-Banden ermittelte, die über Onlinebanking-Kunden versuchten mit Schadsoftwareplatzierung Bankkonten zu plündern. Doch das Bundesstrafge-

richt in Bellinzona hat Klarheit in den Zuständigkeitsdschungel gebracht, demnach muss die Bundesanwaltschaft auch den aus dem Ausland, vermutlich aus Russland operierenden Hintermännern nachgehen und nicht nur den in der Schweiz ansässigen Mittätern.

Seit dem 1. Januar 2012 hat die Schweiz die Europaratskonvention über die Cyberkriminalität ratifiziert. Sie hat sich damit verpflichtet, Computerbetrug, Datendiebstahl, Fälschung von Dokumenten mittels Computern oder das Eindringen in ein geschütztes Computersystem unter Strafe zu stellen. Die Vertragspartner müssen ausserdem Kinderpornografie und Verletzungen der Urheberrechte im Internet bestrafen. Diese Ratifizierung erfordert Anpassungen des Strafgesetzbuches, Klarheit in den Zuständigkeiten und auch eine eigene Cybercrime-Bekämpfungsstelle.

Letzteres übernimmt die in der Schweiz KOBIK (Koordinationsstelle zur Bekämpfung der Internetkriminalität). Die KODIK hat in ihrem Jahresbericht 2010 einen Anstieg von Wirtschaftskriminalität beobachtet, so fanden im Jahr 2010 verschiedenen Wellen von Pishing- Attacken gegen Banken- aber auch Übermittlungsdienstleister statt. KOBIK ermittelt aber zur Hauptsache nicht gegen Wirtschaftskriminalität sondern gegen Kinderpornografie

Die zunehmende Herausforderung in der Bekämpfung von Cybercrime liegt darin, dass die Untersuchungsbehörden spezifisches Fachwissen brauchen, um die Cyberkriminalität zu bekämpfen. Ein Cyber Cop ist ein komplett anderer Typ als ein normaler Ermittler. Er ist vielmehr ein Computerfreak als ein Polizist, muss selber findungsreich sein, um die möglichen Angriffsszenarien der Cyberkriminalität zu begreifen. Und nicht nur das, der Cyber Cop muss sich nicht nur mit kriminellen Elementen auseinander setzen, zunehmend sind auch ganz unbedarfte Internetnutzer im Fokus der Untersuchung, wenn sie nämlich über soziale Netzwerke Firmengeheimnisse unbedacht ausplaudern, oder unbemerkt als Zugang für Schadware benutzt werden.

Mit der raschen Verbreitung von Smartphones, Netbooks und Tablet-PCs wird diese Bedrohung noch zusätzlich angeheizt, denn dadurch wird die ungeschützte Angriffsfläche für Cyber-Kriminelle vergrössert.

Cyberkriminalität wird uns mit Sicherheit in Zukunft immer mehr beschäftigen!

Einziger Trost bei dieser eher düsteren Ausgangslage ist, dass die Bekämpfung der Cyberkriminalität auch wieder neue Arbeitsweisen, Dienstleistungen und Verhaltensmechanismen generiert. Wir dürfen also gespannt sein, ob und wie wir in Zukunft das bis dato ungelöste Problem in den Griff bekommen. Wir halten Sie auf dem Laufenden. ◀