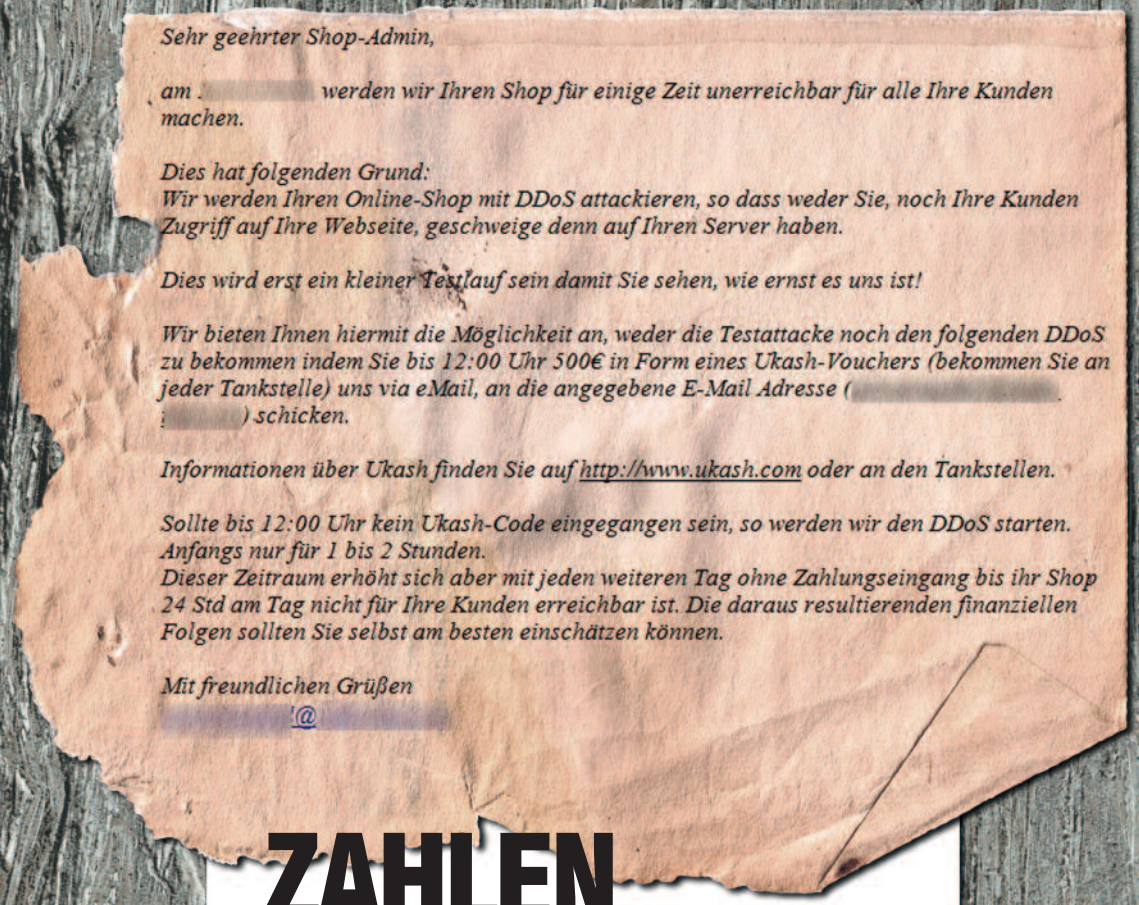

Sehr geehrter Shop-Admin,

am . werden wir Ihren Shop für einige Zeit unerreichbar für alle Ihre Kunden machen.

Dies hat folgenden Grund:
Wir werden Ihren Online-Shop mit DDoS attackieren, so dass weder Sie, noch Ihre Kunden Zugriff auf Ihre Webseite, geschweige denn auf Ihren Server haben.

Dies wird erst ein kleiner Testlauf sein damit Sie sehen, wie ernst es uns ist!

Wir bieten Ihnen hiermit die Möglichkeit an, weder die Testattacke noch den folgenden DDoS zu bekommen indem Sie bis 12:00 Uhr 500€ in Form eines Ukash-Vouchers (bekommen Sie an jeder Tankstelle) uns via eMail, an die angegebene E-Mail Adresse ( ) schicken.

Informationen über Ukash finden Sie auf http://www.ukash.com oder an den Tankstellen.

Sollte bis 12:00 Uhr kein Ukash-Code eingegangen sein, so werden wir den DDoS starten. Anfangs nur für 1 bis 2 Stunden.
Dieser Zeitraum erhöht sich aber mit jeden weiteren Tag ohne Zahlungseingang bis ihr Shop 24 Std am Tag nicht für Ihre Kunden erreichbar ist. Die daraus resultierenden finanziellen Folgen sollten Sie selbst am besten einschätzen können.

Mit freundlichen Grüßen
@

ZAHLEN ODER PLEITEGEHEN?

Mario Fischer

Dass die Online-Kriminalität immer weiter steigt, ist kein Geheimnis. Phishingversuche, gefälschte Mails, das Unterschieben von Trojanern – das alles zielt im Wesentlichen auf die Unachtsamkeit oder Unerfahrenheit von Nutzern ab. Von Erpressungen an Betreibern großer Websites oder Online-Shops liest man schon seltener. Dass mittlerweile gerade auch kleine Shops Opfer skrupelloser Erpresser werden – davon hört man fast gar nichts. Niemand will darüber sprechen, weil verständlicherweise die Angst vor der DDoS-Mafia umgeht. Wen es erwischt, der kann seinen Online-Laden möglicherweise zusperren. Aber: Kann man sich auch erfolgreich wehren?

Sie kommen zwar grammatikalisch ungelenk, aber doch freundlich daher. Verkürzt heißt es per E-Mail: „Sehr geehrter Shop-Admin, gibt uns 500 Euro oder wir sprengen Deinen Shop elektronisch in die Luft. Mit freundlichen Grüßen, Ihr Erpresser." Wow! Wie reagiert man darauf? Ignorieren ist eine denkbar schlechte Idee, denn man meint es in der Regel sehr ernst und weist das auch ein paar Tage später nach, indem man den Shop erst mal nur für eine Stunde lahmlegt. Nun glaubt man dem Mailschreiber. Aber die Frage „Wie reagiere ich nun?" bleibt trotzdem bestehen. Zahle ich und mache mich ab jetzt für die Zukunft erpressbar? Wann kommt die nächste Zahlungsaufforderung – und wie viel Geld wird man beim zweiten Mal verlangen, wenn ich beim ersten Mal anstandslos gezahlt habe? Was passiert, wenn ich nicht zahle? Nun – ganz einfach: Dann wird mit professionellen Methoden eine Attacke gegen den Shop gestartet und er ist dauerhaft nicht mehr erreichbar. Was aber viel, sehr viel wahrscheinlicher ist: Der Provider nimmt den Shop sofort aus dem Netz, denn eine solche Attacke betrifft auch ganz massiv aller anderen dort gehosteten Websites und Online-Shops. Eine ausweglose Situation?

Abb. 1: Ukash warnt selbst vor betrügerischen Mails

Die Erpresser arbeiten hochprofessionell

Zunächst einige kurze Erläuterungen, wie die DDos-Mafia operiert. DDos steht für Distributed Denial of Service und dahinter verbirgt sich ein (räumlich) verteilter Angriff von unterschiedlichen Rechnern auf einen Webserver. Kommen mehr Anfragen gleichzeitig, als der Webserver oder die davorliegende Infrastruktur bewältigen kann, stellt dieser seinen Dienst erst einmal ein bzw. seine Antworten verzögern sich so lange, dass echte Benutzer ein sog. Time-out bekommen, also eine Fehlermeldung. Oft werden auch fehlerhafte Anfragepakete an den Server geschickt, um ihn zusätzlich zu belasten, oder man nutzt bekannte Sicherheitslücken aus, um ihn gezielt zum Absturz zu bringen. Nach dem automatischen Neustart legt ihn dann gleich das nächste eintreffende Datenpaket wieder lahm. In der Regel erfolgt der Angriff direkt auf TCP/IP-Ebene, denn damit lassen sich leichter sehr viel mehr Pakete erzeugen als über Applikationsaufrufe.

Ziel ist es, die technische Infrastruktur so zu überlasten, dass keinerlei Anfragen mehr beantwortet bzw. Webseiten ausgeliefert werden können. In der Regel sind, wie oben erwähnt, immer mehrere Websites betroffen, je nach den internen Strukturen und der Größe des Providers möglicherweise auch alle betreuten Webauftritte. Eine Firewall nützt für solche Attacken leider herzlich wenig, denn sie soll ja unberechtigte Eindringversuche von außen stoppen – die Anfragen an einen Webserver sind aus Sicht der Firewall ja aber berechtigte bzw. erwünschte Eingangssignale und daher werden sie durchgelassen. Ist ein Angriff sehr massiv, werden oft, wie bereits erwähnt, schon die Leitungen derart überlastet, dass bereits vor der Firewall eine Verstopfung eintritt. Bei reinen TCP/IP-Angriffen ist die Firewall nicht nur nicht hilfreich, sie wird durch die Überlastung mit Datenpaketen sogar selbst zum Blockade-Problem.

Wie kommen die Erpresser unerkannt an Ihr Geld? Auch hier hilft das Web. Der Wunsch vieler Surfer, bestimmte Angebote im Web auch wirklich anonym (und sicher) bezahlen zu können, hat einige Anbieter hervorgebracht, die genau dies als Geschäftszweck haben. Das Prinzip ist dabei einfach. Man kauft gegen Bargeld einen Voucher, mit dem man überall da im Web einkaufen kann, wo dieses System als Zahlungsmethode angeboten wird. Solche Voucher werden mittlerweile sogar an Tankstellen angeboten und sind somit leicht zu bekommen. Die Erpresser fordern nun den Code des Vouchers per Mail an eine nicht rückverfolgbare E-Mail-Adresse zu schicken, die natürlich in regelmäßigen Abständen gewechselt wird und aus dem fernen Ausland kommt – in der Regel aus Ländern, mit denen die deutsche Polizei nicht in ständigem und kooperativem Austausch steht. Somit hinterlassen die Erpresser keine oder nur wenig auswertbare Spuren. Und ihnen kommt der Zeitdruck zugute, denn sie setzen kurze Reaktionsfristen. Ein Anbieter eines solchen anonymen Vouchersystems ist beispielsweise der in London ansässige Dienst Ukash (*www.ukash.com*), dessen Kunden offenbar mittlerweile selbst Opfer von betrügerischen Mails werden, wie eine Pop-up-Meldung auf der Website zeigt. Natürlich haben Ukash und andere Anbieter selbst mit den kriminellen Machenschaften der Erpresser nichts zu tun. Aber die von ihnen gebotene Ano-

nymität schützt in diesem Fall natürlich eben auch Betrüger, die sich leicht dahinter verstecken können.

Wird nicht gezahlt, kommt zunächst zur Warnung und zum Beweis, dass man in der Lage ist, den Shop tatsächlich lahmzulegen, ein kurzer Angriff. Dieser soll dem Betreiber zeigen, wie ernst das Ganze ist und dass es sich nicht um eine Spaßmail von Skriptkiddies handelt. Der Angriff selbst kommt dann geografisch verteilt von verschiedenen Rechnern, sodass man nicht einfach einige IP-Adressen wegfiltern kann.

Unerfahrene Surfer sind die Steigbügelhalter der Erpresser

Wie kommt man an so viele Rechner weltweit, um solche verteilten Angriffe überhaupt realisieren zu können? Das ist mittlerweile leider relativ einfach. Im Web gibt es für einige Hundert Euro Bau-

> „Fatal: Je mehr Anonymität für Netzteilnehmer von politischer Seite gefordert und realisiert wird, umso leichter macht man es auch Betrügern und Erpressern, unerkannt zu bleiben.

kästen zu kaufen, mit denen man sich eigene Trojaner zusammenklicken kann. Man kann so z. B. einen Trojaner (Software, die sich vom Nutzer unbemerkt auf seinem Rechner einnistet und es ermöglicht, bestimmte Aktionen von dort aus ohne Wissen des Nutzers zu starten) in einem Bild oder einem PDF verstecken und per E-Mail verschicken. Jeder, der dann dieses Bild oder generell den Anhang öffnet und keine aktuelle Schutzsoftware installiert hat, holt sich damit ungewollt den Zugang für Fremde auf das eigene System. Der Trojaner „meldet“ sich nach der Installation bei einem zentralen Steuerungssystem im Internet und wird dort registriert. Benötigt man Zugang zu dem Rechner, funkt das zentrale System (das durchaus ebenfalls physikalisch verteilt sein kann) ihn an und veranlasst den zum Zombie mutierten Computer, bestimmte Dinge zu tun, z. B. in diesem Fall im Abstand von

INTERVIEW mit Johannes Klinger Websale AG

Website Boosting: Herr Klinger, Sie hatten als großer Anbieter von Shop-Mietlösungen ja bereits gezielte DDoS-Attacken auf Ihre Kunden abzuwehren. Welche Maßnahmen haben Sie hierfür vorab in Betracht gezogen und dann realisiert?

Johannes Klinger: Als die erste Attacke auf einen Shop erfolgte, konnte diese damals noch mit vorhandenen Mitteln nach einiger Zeit abgewehrt werden. Die Analyse des Angriffs zeigte jedoch erweitertes Gefahrenpotenzial und dass herkömmliche Firewalls, egal ob Hard- oder Software, vollkommen ungeeignet sind, solche Angriffe abzuwehren. So wurden vorsorglich Hersteller spezialisierter DDoS-Abwehrsysteme kontaktiert, Systeme bewertet und verglichen. Mangels einer echten Überprüfbarkeit der Wirksamkeit konnte jedoch noch keines der Systeme vorsorglich angeschafft werden, da die Kosten für Hardware, Software und Softwarewartung sowie Schulung und Administration bei größeren zu schützenden Infrastrukturen wie bei uns weit im sechsstelligen Bereich liegen. Als einige Monate später ein anderer DDoS-Angriff startete, diesmal eindeutig mit einer Erpressung als Hintergrund, konnten zwei von uns favorisierte Systeme, eines aus Europa, eines aus den USA, bestellt werden. Sofort nach der Anlieferung des ersten Systems mitten in der Nacht wurde es installiert und „live“ getestet. Bei etlichen folgenden, äußerst massiven Angriffsversuchen mit Dutzenden unterschiedlichster Methoden und einer steigenden Dauer und Intensität bis zu drei vollen Tagen stellte sich ein System als besonders effizient in der Abschwächung der Angriffe heraus. Folglich wurde ein solches System angeschafft, welches entsprechend für unser Gesamtnetz ausgelegt wurde.

Das hört sich nach sehr viel Aufwand an. Wäre es denn nicht doch wirtschaftlicher gewesen, den betroffenen Shop einfach für die Zeit der Angriffe vom Netz zu nehmen?

Kurzfristig wirtschaftlicher ist das für einen Hoster sicher – vor allem für einen Hoster, der überwiegend nach dem oft geforderten Motto „möglichst billig“ hostet und nicht nach dem Motto „möglichst gut“. Es ist sehr einfach, die Verantwortung an den Kunden abzugeben und abzuschalten. Deshalb wird es auch genauso praktiziert. Die meisten Hoster verstehen sich auch als Web-Hoster und nicht als spezialisierte Shop-Hoster mit Firmenkunden, die von ihrem Shop leben. Abschalten bedeutet aber 100 % Umsatzausfall für den betroffenen

Millisekunden eine bestimmte Webadresse, die des Shops, aufzurufen. So ist es möglich, innerhalb kurzer Zeit über Tausende oder gar Millionen solcher ferngesteuerter Rechner massive Anfragen an einen Server zu generieren. Der Besitzer eines solchen Zombiesystems bekommt davon in der Regel rein gar nichts mit. Wem der Aufbau eines eigenen Zombienetzwerkes zu aufwendig ist, der kann im Untergrund solche Netze auch kostengünstig mieten. Die Bezahlung erfolgt prinzipiell über die gleichen anonymen Zahlungssysteme.

Mittlerweile grassieren offenbar auch einige Trojaner, die den Rechner des Benutzers lahmlegen und keine Eingaben mehr zulassen. Es erscheint eine Meldung, dass es sich hierbei um eine Art „Online-Durchsuchung" des Rechners vom Bundeskriminalamt handelt und dass man kinderpornografisches Material auf diesem Rechner gefunden hätte. Wahrscheinlich wird der Trojaner in Bilddateien in entsprechenden Foren gepackt, damit man möglichst treffsicher an die „Zielgruppe" herankommt, die Meldung dadurch glaubwürdiger erscheint und vor allem bei Nutzern landet, die den Gang zur Polizei aus einsehbaren Gründen scheuen. Es heißt dann, eine „Geldstrafe" über 100.- € würde fällig und nach Zahlung über einen Ukash-Gutschein und Übermittlung an die Maildomain „bundeskriminalamtes.org" werde der Rechner wieder freigeschaltet. Hiervor warnt Ukash mittlerweile (siehe Abbildung 1) auch auf seinen Webseiten.

„Was tun?", sprach Zeus

Experten und auch die zuständigen Stellen bei der Kripo raten dringend davon ab, einfach zu zahlen. Wer einmal zahlt, wird auch ein zweites Mal zahlen – das vermuten bzw. wissen auch die Erpresser. Im Prinzip verschiebt man das Problem damit nur und es schlägt beim zweiten Mal möglicherweise umso heftiger zu, z. B. genau in der Weihnachtszeit, wo die meisten Shops nicht selten die Hälfte ihres Jahresumsatzes generieren. Man sollte hier keinen Raum für falsche Scham vor Imageverlusten lassen und in jedem Fall sofort die Kriminalpolizei einschalten. Dort behandelt man grundsätzlich solche Dinge sehr diskret und es gibt mittlerweile auch Experten, die in letzter Zeit immer häufiger mit solchen Fällen zu tun haben. Zwar führen Nachforschungen über die Herkunft der Angriffe meist ins Leere bzw. ergeben keine konkreten Anhaltspunkte. Aber bei der Kripo kennt man gleiche oder ähnlich gelagerte Fälle und man wird gut beraten, wie im Einzelfall zu reagieren ist. Und: Solche Meldungen erlauben es der Polizei nicht zuletzt auch, durch Erkennung gewisser Muster kon-

Online-Shop und nicht nur Ausfall von ein paar Webseiten. Und es bedeutet, einen Kunden, der selbst fachlich keine Chance hat, dem Angriff zu begegnen, „im Regen stehen zu lassen" oder ihm exorbitante Kosten für die Schutzmaßnahmen für seinen eigenen Shop aufzubürden. Wir verstehen uns aber als Dienstleister mit dem Ziel, unseren anspruchsvollen Kunden stets maximalen Umsatz und stets funktionierenden Shopbetrieb zu ermöglichen. Daher ist für uns so ein exklusiver umfassender Schutz Ausdruck unserer Verantwortung für den laufenden Betrieb aller bei uns gehosteten Shops, egal, ob etwas kleiner oder ganz groß. Nach unserer Kenntnis sind wir seitdem der erste und einzige Shop-Hoster in Deutschland, der präventiv alle gehosteten Shops unter einen hochwirksamen DDoS-Schutzschirm genommen hat und so allen seinen Kunden, den Online-Händlern, den bestmöglichen Schutz vor Erpressungen bietet.

Was würden Sie Shopbetreibern aus Ihrer Erfahrung heraus raten, die mit solchen Erpressungen in Berührung kommen?

Zahlen Sie keinesfalls. Sie öffnen Folgeerpressungen Tür und Tor. Gehen Sie zur Polizei, auch wenn dieser teilweise aufgrund von Datenschutzbestimmungen oder fehlender internationaler Kooperationsverträge manchmal entscheidende Informationen oder Handhabe fehlen. Die Chance, den Kriminellen das Handwerk zu legen, muss gewahrt werden und nur umfassende Kenntnis aller Erpressungsfälle kann deren Austrocknung bewirken.

Haben Sie einen Tipp für Online-Händler, bei denen der Vertrieb über Internet spürbare Umsatzanteile bringt?

Prüfen Sie, ob Sie es sich leisten können oder wollen, im Ernstfall bei einer DDoS-Erpressung mehrere Tage oder Wochen offline zu sein oder dauerhaft Erpressungsgeld zu zahlen. Wenn Sie das nicht wollen, ist es klug, im Vorfeld zu handeln. Erpresser sind Leute, die in der Regel schnell und bequem Geld erlangen möchten. Sie suchen sich daher die Opfer, bei denen sie das leichteste Spiel haben. Machen Sie es daher dem Erpresser schwer, Sie mit DDoS zu erpressen, indem Sie ihren Shop schützen oder schützen lassen. So werden Sie mit hoher Wahrscheinlichkeit dauerhaft Ruhe vor Erpressern haben.

Vielen Dank!

Johannes Klinger ist Vorstand der Websale AG und verfügt über mehr als 15 Jahre Erfahrung im Entwickeln, Betreiben und Hosten von Shoplösungen. Zu den Kunden zählen Versandhändler aus allen Branchen mit nationaler und internationaler Ausrichtung.

> Bei einmaligen Zahlungen wird es in der Regel nicht bleiben.

zentrierter und im Verbund gegen solche Machenschaften vorzugehen.

Ein einzelner Shopbetreiber ist in der Regel völlig damit überfordert, wie man technisch erfolgreich gegen solche Attacken vorgehen kann. Das ist auch weder seine Aufgabe noch sein Business. Es empfiehlt sich daher, sofort mit dem Provider Kontakt aufzunehmen, bei dem der Shop physikalisch betrieben wird. Zu klären ist dann primär, ob dieser bereits Schutzsoft- oder -hardware installiert hat, die mit solchen Angriffen umgehen kann. Gerade bei kleineren und mittleren, aber auch bei größeren Providern ist das leider oft nicht der Fall, denn der Einsatz solcher Filtermechanismen ist sehr aufwendig und damit teuer. Und präventiv und ohne konkreten Anlass schnell mal fünfzig- oder hunderttausend Euro zu investieren, widerspricht eben oft den betriebswirtschaftlichen Preiskalkulationen der Provider. Daran dürfte die „Wo-kann-ich-am-billigsten-hosten?"-Einstellung der Shopbetreiber nicht ganz unschuldig sein. Zudem ist der Markt für Lösungen laut Johannes Klinger, Vorstand der Websale AG, nicht gerade transparent (siehe Interview). Es ist klar, dass jeder Anbieter auf seinen Websites das eigene System über den grünen Klee lobt – aber was sie dann tatsächlich zu leisten in der Lage sind, steht auf einem ganz anderen Blatt. Das Problem ist dabei, dass man gar nicht die Zeit hat, umfassend nach den besten Lösungen zu recherchieren.

Daher sucht sich ein Teil der Erpresser eben genau den Mittelstand als Angriffsziel aus. Große Anbieter wie Amazon, Otto oder Apple kann man zwar mit professionellen Mitteln ebenfalls via DDoS-Attacken angreifen und auch höhere Summen verlangen – aber man hat es hier mit aus technischer Sicht ungleich professionelleren Gegenspielern zu tun, die zudem bedeutend mehr Finanzpower und -spielraum im Hintergrund haben. Kriminaloberkommissar Michael Büchel, der bei der Polizei Nürnberg für Cybercrime zuständig ist, schätzt, dass die Dunkelziffer derartiger Erpressungen wahrscheinlich mittlerweile relativ hoch ist. Strafanzeigen gingen dagegen bisher nur sehr wenige ein. Hier dürfte wahrscheinlich die Angst des Shopbetreibers dominieren, dass vielleicht bekannt würde, man hätte irgendeine Art Sicherheitslücke. Möglicherweise wägt man auch ab, lieber ein paar Hundert Euro zu zahlen, weil das als einfachster Weg erscheint, die drohende Gefahr abzuwehren. Er empfiehlt, sich in jedem Fall an die zuständige Polizeidienststelle zu wenden; von dort würde man an die darauf spezialisierten Stellen verwiesen. Die Experten der Kripo setzen sich dann in der Regel schnell mit dem Provider in Verbindung und versuchen, Beweise zu sichern. Da Erpressung kein Kavaliersdelikt darstellt, würde hier auch entsprechend massiv und ernsthaft reagiert. Die Behörden sind auch in der Lage, zum Teil länderübergreifend z. B. Überwachungsmaßnahmen für E-Mail-Accounts durchzusetzen. Auf die Frage, wie denn die Täter über die Codes zu Bargeld gelangen, weiß Büchel, dass dies kein nennenswertes Problem darstellt. Entweder kauft man leicht wiederverkaufbare Produkte in Shops ein, die solche Voucherzahlungen anbieten, oder es wird über Online-Casinos „gewaschen". Dort wird der Voucher zunächst in Spielchips getauscht und nach ein paar Spielen lässt man sich das Gros der übrig gebliebenen Chips einfach auszahlen.

TIPPS!

- Sorgen Sie dafür, dass Sie übliche Mailadressen wie „admin@", „info@" und „webmaster@" auch **wirklich** erhalten, auch wenn darüber oft Spam empfangen wird.
- Kontaktieren Sie **sofort** Ihren Provider und sprechen Sie mit ihm mögliche Abwehrmaßnahmen durch.
- Falls Ihr Provider keinen Schutz bieten kann oder will, sollten Sie sich **rechtzeitig** darum kümmern, ggf. zumindest übergangsweise zu wechseln.
- Kontaktieren Sie **in jedem Fall** auch die Kriminalpolizei

Büchel gibt weiterhin zu bedenken, dass es wahrscheinlich nicht bei einer einmaligen Zahlung bleibt. Da sich die Täter meist in diversen, zugangsgeschützten Untergrundforen austauschen, kann ein zahlender Shopbetreiber schnell plötzlich auch von anderen Tätern ins Visier genommen werden. Oder die Adressen von Shops mit Zahlungsbereitschaft werden möglicherweise einfach auch weiterverkauft. Eine fatale Spirale, denn je mehr Betroffene klaglos zahlen, desto attraktiver wird dieses Feld für die Online-Betrüger. Man darf also getrost davon ausgehen, dass sich die Fälle in Zukunft sogar noch häufen werden, denn jede Zahlung stärkt natürlich die finanziellen und damit technischen Möglichkeiten der Betrüger.

Es bleibt abzuwarten, wie die Branche mit diesem für den einzelnen Betreiber durchaus existenzbedrohenden Problem umgehen wird. Vielleicht sollten oder müssen hier auch die entsprechenden Verbände tätig werden und gemeinschaftlich funktionierende Abwehrmechanismen entwickeln, die bei Erpressungsversuchen schnell und flexibel einsetzbar sind. Das würde es für die Erpresser auf Dauer weniger lukrativ machen. ¶