Fehler bei Hostern gefährden die Sicherheit von DKIM

[expand title="mehr lesen…"]

Fehler bei Hostern gefährden die Sicherheit von DKIM

Wissen Konfigurationsfehler bei DKIM

Bild: Thorsten Hübner

DKIM-Fail

Fehler bei Hostern gefährden die Sicherheit von DKIM

Online-Kriminelle versenden regelmäßig E-Mails unter falschem Namen, um Nutzer zur Herausgabe von sensiblen Daten zu bewegen. Mit DKIM sind Spam-Filter in der Lage, solche gefälschten Mails zu erkennen. Doch unsere Analysen zeigen, dass einige Webhoster mit Fehlkonfigurationen Spammern und Phishern Tür und Tor öffnen. Von Leo Dessani und Jan Mahn

Eine neue E-Mail vom Chef. Laut Mailprogramm stammt sie auch von seiner Adresse. Offenbar steckt er im Ausland in Schwierigkeiten, hat seine Kreditkarte verloren und braucht schnell etwas Geld vom Firmenkonto. Was auf den ersten Blick wie eine authentische E-Mail aussieht, kann sich beim zweiten Blick als Phishing-Versuch offenbaren. Ist die gefälschte Mail gut gemacht, kann sie Filter wie SpamAssassin mit einiger Wahrscheinlichkeit umgehen und landet direkt im Posteingang des Nutzers. Aber selbst wenn der Nutzer vorsichtig ist und die E-Mail-Adresse des Absenders beim Öffnen gewissenhaft prüft, ist das keine Garantie, dass die Nachricht auch tatsächlich von dieser Adresse stammt.

Kriminelle verfolgen mit Phishing-Mails ein konkretes Ziel: das Vertrauen der Nutzer zu gewinnen und sie zu animieren, vertrauliche Daten wie Passwörter preiszugeben (Social Engineering). Senden die Täter ihre Phishing-Mails von einer echten E-Mail-Adresse einer Organisation, auf die sie selbst keinen Zugriff haben, gewinnen sie potenziell mehr Vertrauen der Nutzer, denn vielen Anwendern ist nicht bewusst, dass man Absenderadressen leicht fälschen kann. Möglich ist das durch eine konzeptionelle Schwachstelle im SMTP-Protokoll: Einen Mechanismus für die Authentifizierung der Absenderadresse gibt es im Protokoll selbst nicht.

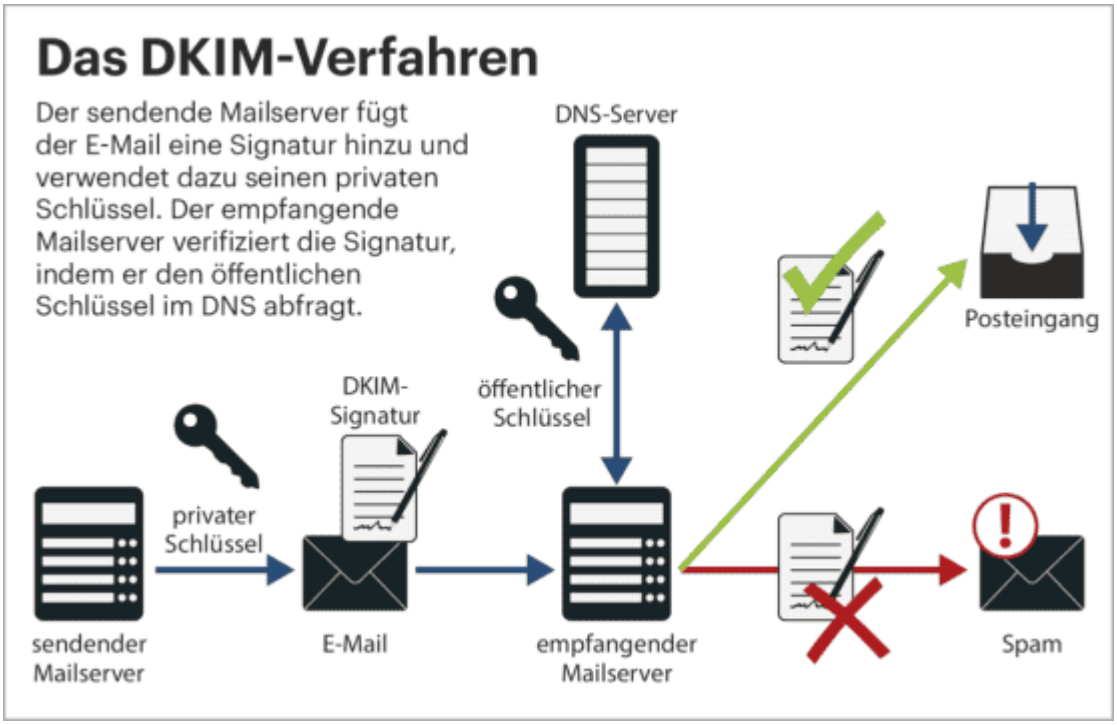
Bereits 2004 haben sich Yahoo und Cisco zusammengeschlossen

und gemeinsam einen Standard konzipiert, der das Problem lösen soll: „DomainKeys Identified Mail“ (DKIM). Seit 2011 ist DKIM als Internetstandard von der Internet Engineering Task Force (IETF) anerkannt und wird von vielen Mailserverbetreibern eingesetzt. Das Fälschen von Absenderadressen (Mail-Spoofing) soll dadurch erschwert werden, dass jeder ausgehenden E-Mail eine digitale Signatur als Mail-Header beigefügt wird. Die Signatur im Header kann vom empfangenden Mailserver validiert werden. Mails mit gefälschter Absenderadresse können so erkannt und markiert oder entsorgt werden. Wie DKIM im Detail funktioniert, erfahren Sie im Kasten rechts.

DKIM: Mit Signaturen gegen Betrüger

DKIM ist ein Standard, um die Echtheit der versendenden Domain einer E-Mail zu prüfen. Anders als zum Beispiel PGP ist für DKIM der Betreiber des Mailservers verantwortlich – als Nutzer kann man das Verfahren nicht einrichten. Ein Serverbetreiber, der DKIM-Signaturen an seine Mails anhängen möchte, generiert ein Schlüsselpaar aus öffentlichem und privatem Schlüssel. Um den öffentlichen Schlüssel bekannt zu machen, kommt DNS zum Einsatz: Den öffentlichen Schlüssel legt der Administrator als TXT-Record in der DNS-Zone seiner Domain ab. Der private Schlüssel darf den Mailserver nicht verlassen.

Beim Versenden von Mails werden zwei Prüfsummen berechnet: eine für ausgewählte Teile des Headers, eine für den Body der Mail. Die Prüfsummen werden mit dem privaten Schlüssel per RSA signiert und als Mailheader DKIM-Signature der E-Mail beigefügt, ergänzt um weitere Informationen. Zu denen zählen unter anderem die Absender-Domain, die Namen aller signierten Header-Felder sowie der sogenannte Selektor. Der Selektor entspricht dem Namen des DNS-Eintrags, in dem der öffentliche Schlüssel liegt. Die Liste der mitsignierten Header-Felder muss mindestens das Feld From: enthalten, also die Absenderadresse, die auch dem Empfänger angezeigt wird. So ist sichergestellt, dass nachträgliche Manipulationen die Signatur ungültig machen.



Empfängt ein Mailserver eine digital signierte E-Mail und ist der Server so eingerichtet, dass er DKIM prüft, fragt er aus dem DNS für die angegebene Domain den öffentlichen Schlüssel mit dem Namen des Selektors ab. Mit dem öffentlichen Schlüssel kann er die Echtheit der digitalen Signatur bestimmen. Ist die Prüfung erfolgreich, ist gewährleistet, dass die E-Mail von einem authentischen Absender stammt und nicht verändert wurde. Schlägt sie fehl, kann das ein Indiz dafür sein, dass die E-Mail gefälscht ist. Was dann passiert, kann der Betreiber des empfangenden Servers bestimmen. Oft führt das Scheitern zur sofortigen Ablehnung der E-Mail, manchmal wird sie nur als Spam-verdächtig markiert. Das Ergebnis der Prüfung fügt der empfangende Mailserver mit dem Header Authentication-Results an die Mail an. dkim=pass zeigt an, dass die Prüfung erfolgreich war, dkim=fail, dass sie fehlschlug.

Fast alle Mailserver verlassen sich nicht auf eine Methode zum Filtern allein und schalten mehrere Filter in Reihe. Mit Inhaltsfiltern reagieren sie zum Beispiel auf typische Spam-Begriffe wie „Casino“ und „Viagra“. In solchen Umgebungen vergibt jeder Filter einen Punktwert für die Einordnung der Mail – überschreitet die Summe aller Punkte einen Schwellwert, wird die Mail aussortiert oder markiert. Eine erfolgreiche

DKIM-Prüfung wirkt sich in vielen Konfigurationen positiv auf die Vertrauenswürdigkeit aus und zieht Punkte ab.

Geteilte Server

Seit einigen Jahren bieten immer mehr Webhosting-Anbieter ihren Kunden das Signieren von E-Mails mit DKIM an. Bei einigen Providern ist DKIM sogar standardmäßig für alle Domains aktiviert, bei anderen reicht ein Klick im Kundencenter, um DKIM für einzelne oder alle Domains zu aktivieren. Die Hoster machen es den Kunden leicht und übernehmen das Hantieren mit Schlüsseln und DNS-Einträgen. Ohne Zutun des Kunden erstellen sie ein Schlüsselpaar, legen den öffentlichen Schlüssel im DNS als TXT-Record ab und richten den privaten Schlüssel auf dem Mailserver ein. Fortan werden alle ausgehenden E-Mails automatisch mithilfe von DKIM signiert.

Bei Webhosting-Paketen sind sogenannte Shared Server verbreitet. Mehrere Kunden teilen sich einen Server, also dessen Ressourcen und Software. Dadurch kann der Anbieter mehr Kunden bedienen, als er tatsächlich physische Server vor Ort hat. Bei solchen Shared Servern muss gewährleistet sein, dass ein Kunde nicht auf die Daten eines anderen zugreifen kann. Für die Webseitendaten und Datenbanken funktioniert das auch sehr zuverlässig.

DMARC: Das Anti-Spam-Trio

Neben DKIM existieren zur Bekämpfung von Spam- und Phishing-Mails zwei weitere Verfahren: Sender Policy Framework (SPF) und Domain-based Message Authentication (DMARC).

SPF beruht auf der Annahme, dass alle E-Mails einer Domain von einer festen Anzahl von autorisierten Mailservern versendet werden. In einem TXT-Record veröffentlicht der Administrator die Adressen dieser Mailserver im DNS. Der Spam-Filter auf dem empfangenden Server kann bei der Entgegennahme der E-Mail

durch das Abrufen dieses DNS-Eintrages prüfen, ob der sendende Mailserver zum Verschicken berechtigt ist. Was geschieht, wenn eine E-Mail über einen nicht autorisierten Mailserver versendet wird, kann ebenfalls im DNS-Eintrag festgelegt werden.

DMARC ist keine eigene Technik, sondern kombiniert die Ergebnisse der SPF- und DKIM-Prüfungen: Mit DMARC beschreibt der Administrator, ebenfalls in Form eines DNS-Eintrages, wie der empfangende Mailserver mit einer E-Mail umgehen soll, bei der die SPF- oder DKIM-Prüfungen fehlschlagen, und wen er darüber informieren soll.

Signaturen für fremde Domains

Doch werden auch die privaten DKIM-Schlüssel verschiedener Kunden sauber getrennt? DKIM ist schließlich nur sinnvoll, wenn gewährleistet ist, dass niemand gefälschte Signaturen generieren kann. Was für den Schutz von Kundendaten aufShared Servern gilt, muss auch für Schlüsselpaare gelten: Gültige DKIM-Signaturen auf Grundlage des privaten Schlüssels dürfen ausschließlich für E-Mails generiert werden, die vom Inhaber einer Domain stammen und nicht etwa von anderen Kunden, deren Accounts zufällig auf demselben Server liegen.

Providervergleich

Um herauszufinden, ob Hosting-Anbieter die DKIM-Signaturen ihrer Kunden auf demselben Server sauber trennen, haben wir 37 deutsche Anbieter unter die Lupe genommen und angefragt, ob sie DKIM für ihre Kunden aufShared Servern bereitstellen. Die Antwort: 17 Provider bieten DKIM für ihre Kunden gar nicht an. Vier Provider stellen DKIM nur aufInstanzen bereit, die nicht mit anderen Kunden-Domains geteilt werden (zum Beispiel virtuelle Server oder Managed Server). Übrig blieben 16 Provider für unsere Tests.

DKIM-Konfigurationsfehler bei deutschen Webhostern				
Anbieter	**getestetes Paket**	**DKIM-Unterstützung**	**Ergebnis**	**Reaktion**
All-Inkl.com	Premium	automatisch aktiv	verwundbar	DKIM für die PHP-Mailfunktion deaktiviert
Contabo	Paket L	automatisch aktiv	nicht verwundbar	
creoline	WordPress Hosting S	manuell aktivierbar	verwundbar	Lücke geschlossen
Febas	Professional	manuell aktivierbar	Test nicht möglich[1]	
Hetzner	Level 4	manuell aktivierbar	verwundbar	Lücke geschlossen
hosting.de	Medium	automatisch aktiv	nicht verwundbar	
Hostinger	Premium	manuell aktivierbar	Test nicht möglich[1]	
netclusive	Easy 5.0	manuell aktivierbar	verwundbar	DKIM zunächst deaktiviert, Lücke später geschlossen
netcup	Webhosting 4000	automatisch aktiv	nicht verwundbar	
one.com	Entdecker	automatisch aktiv	nicht verwundbar	
Serverprofis	Private L 5.3	automatisch aktiv	nicht verwundbar	
Strato	Basic	automatisch aktiv	nicht verwundbar	
UD Media	Power 5.0	automatisch aktiv	verwundbar	Lücke geschlossen
webgo	SSD Profi	über den Support aktivierbar	teilweise verwundbar	
webhoster.de	Starter Tarif	manuell aktivierbar	nicht verwundbar	
WebhostOne	Basic	manuell aktivierbar	verwundbar	Lücke geschlossen
[1] keine anderen Kunden mit aktivem DKIM auf demselben Server				

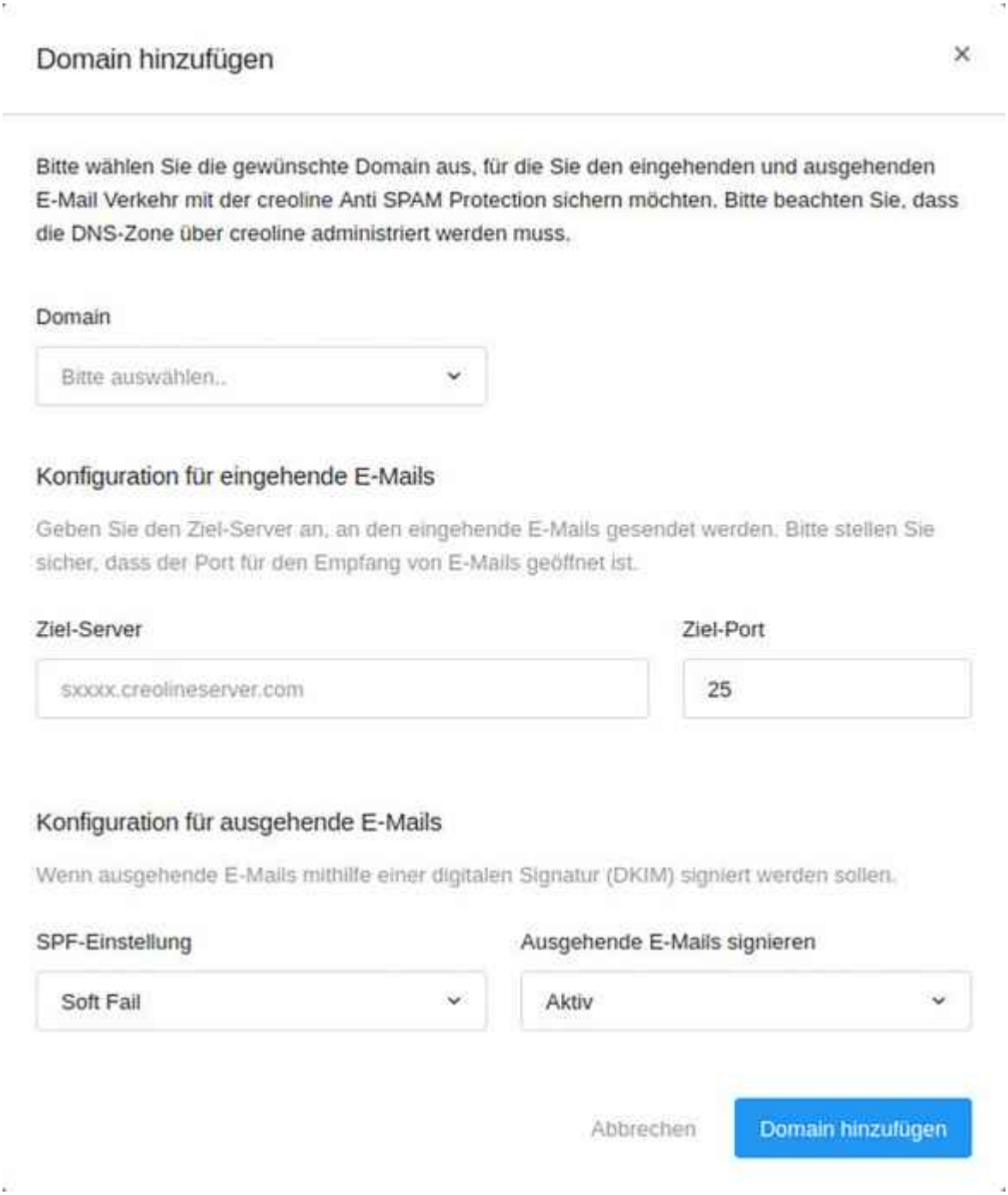
Bei All-Inkl.com, Contabo, hosting.de, netcup, one.com, Serverprofis, Strato und UD Media ist DKIM standardmäßig

aktiviert. Bei einigen Anbietern war es notwendig, DKIM im Kundeninterface einzuschalten. Für unseren Test suchten wir den DKIM-Selektor unserer Test-Domains über die DNS-Einstellungen des Kundenportals. Dann gingen wir auf die Suche nach fremden Domains von anderen Kunden, die sich mit uns einen Server teilten. Diese Recherche ist mit einer Reverse--DNS-Suchmaschine im Internet schnell erledigt, indem man nach der IP der eigenen Domain sucht. Für den Test brauchten wir eine fremde Domain, auf der ebenfalls DKIM aktiv war – ob das der Fall ist, findet man heraus, wenn man deren DNS-Einträge durchsucht. Bei den meisten Anbietern ging das schnell, da die DKIM-Selektoren für alle Domains identisch sind. All-Inkl.com, Hostinger und hosting.de vergeben individuelle DKIM-Selektoren auf Grundlage des Datums, an dem DKIM aktiviert wurde. In diesem Fall war etwas Ausdauer gefragt, da wir die fremden Domains manuell prüfen mussten. Nachdem wir fremde Domains mit aktivierter DKIM-Signatur auf „unseren“ Servern ausfindig gemacht hatten, konnte der Test beginnen.

Hoster ohne DKIM-Unterstützung	
Anbieter	DKIM-Unterstützung
1blu	nicht unterstützt
alfahosting	nicht unterstützt
centron	nicht unterstützt
checkdomain	nicht unterstützt
DM Solutions	nur für Managed Server
dogado	nicht unterstützt
DomainFactory	nicht unterstützt
ESTUGO	nicht unterstützt
goneo	nicht unterstützt
Host Europe	nicht unterstützt
Hostpress	nur für vServer
INWX	nicht unterstützt

Hoster ohne DKIM-Unterstützung	
Anbieter	DKIM-Unterstützung
IONOS 1&1	nicht unterstützt
manitu	nicht unterstützt
Mittwald	nicht unterstützt
OVH	nicht unterstützt
Packagecloud (D&T Internet)	nicht unterstützt
profihost	nicht unterstützt
Raidboxes	nur für vServer
TimmeHosting	nur für vServer
united-domains	nicht unterstützt

In allen getesteten Paketen stand uns PHP zur Verfügung – also nutzten wir die PHP-Funktion mail(), um eine E-Mail mit einer fremden Domain in der Absenderadresse, die auf demselben Server gehostet war wie unsere, an ein externes Postfach zu schicken. Eine glatte Fälschung also, die niemals hätte signiert werden dürfen.



Bei Creoline muss man DKIM im Kundencenter aktivieren. Der Anbieter war beim DKIM-Signaturdiebstahl verwundbar, konnte das Problem nach unserem Hinweis aber abstellen.
Bei sechs von sechzehn getesteten Anbietern war das Experiment erfolgreich: All-Inkl.com, creoline, Hetzner, netclusive, WebhostOne und UD Media hängten eine gültige Signatur mit dem privaten Schlüssel der fremden Domain an, obwohl wir zum Versenden nicht berechtigt waren. Unser empfangender Mailserver stufte die Mail als korrekt DKIM-signiert ein. Bei netclusive betraf dies nur Pakete auf dem Server hst1.ncsrv.de. Neue Pakete auf dem Server hst2.ncsrv.de waren

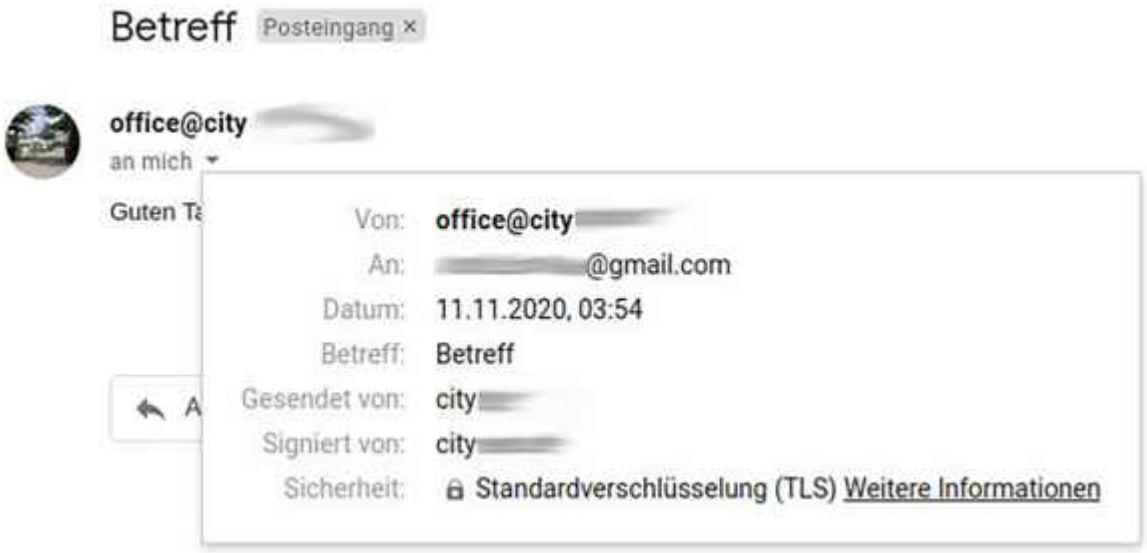
nicht betroffen.

Bei Febas, Hostinger und webgo konnten wir die Recherchen nicht abschließen, weil auf unserem Server keine anderen Domains DKIM aktiviert hatten und somit kein fremdes Schlüsselmaterial zum Testen vorhanden war.

Bei Serverprofis und Strato funktionierte der Angriffsversuch nicht. Beim Versenden aus unserem Account heraus wurde für die fremde Domain entweder eine DKIM-Signatur mit unserem privaten Schlüssel oder gar keine hinzugefügt. Zu einer unbefugt gültigen Signatur kam es nicht. Bei one.com wurden für fremde Adressen gar keine Mails verschickt, ein Angriff war also auch nicht möglich. Bei netcup und hosting.de konnten wir das Problem ebenfalls nicht reproduzieren. Dort werden Mails laut Auskunft des Supports nur dann DKIM-signiert, wenn man sie über den SMTP-Server verschickt und sich bei diesem authentifiziert. Das war hier ein wirkungsvoller Schutz gegen den Angriff.

Vertrauen verspielt

Unsere Untersuchung macht deutlich: Auch wenn das DKIM-Protokoll selbst gut konzipiert ist, haben es einige Webhoster durch fehlerhafte Konfiguration geschwächt. Bei den Anbietern, bei denen wir gefälschte E-Mails versenden konnten, haben wir die Wirksamkeit von DKIM ausgehebelt. Noch mehr: Da wir von einem autorisierten Mailserver verschickten, lieferten auch SPF und damit DMARC keine Fehler. Wir umgingen so auch vergleichsweise streng konfigurierte Spam-Filter und unsere E-Mail landete direkt im Posteingang ohne Spam-Verdacht. Auch sicherheitsbewusste Nutzer, die zum Beispiel mit dem Thunderbird-Plug-in„DKIM Verifier“ arbeiten, das bei jeder Mail das Ergebnis der Signaturprüfung prominent anzeigt, wären auf den Angriff hereingefallen.



Google Mail zeigt an, dass die Mail korrekt signiert wurde. Dabei wurde sie nicht von einem berechtigten Absender verschickt.
Für Spammer und Phisher ist dieser lockere Umgang mit den DKIM-Schlüsseln der Kunden ein großzügiges Angebot, gegen das Betreiber von Maileingangsservern und die Mailempfänger nichts tun können. Abhilfe schaffen können bei dem Problem nur die Hosting-Anbieter.

Nach unseren Experimenten kontaktierten wir die betroffenen Anbieter All-Inkl.com, creoline, Hetzner, netclusive, WebhostOne und UD Media und wiesen auf das Problem hin. Die Hoster, bei denen kein Test möglich war, wiesen wir darauf hin, dass das Problem möglicherweise auch bei ihnen besteht. Webgo bestätigte, dass die Lücke tatsächlich auf einigen Servern existiert – diese ältere Infrastruktur werde in nächster Zeit aktualisiert.

Creoline reagierte schnell mit einer Stellungnahme und wies zunächst darauf hin, dass Versuche, die Absenderadresse zu ändern, spätestens nach fünf Versuchen automatisch unterbunden wurden. Am nächsten Tag hatte man das Problem dann vollständig gelöst und die Manipulation war gar nicht mehr möglich. Netclusive antwortete einen Tag nach dem Hinweis, dass man DKIM vorübergehend ganz abgeschaltet habe, eine Woche später hatte man das Problem dann gelöst und DKIM wieder aktiviert.

Auch bei Hetzner konnte man das Problem bestätigen und stufte es als „mittelschwer“ ein – einen Tag nach der Meldung hatte man den Fehler beseitigt. Weil der Kunde DKIM selbst aktivieren muss, seien nach Angaben von Hetzner nur etwa fünf Prozent der Webhosting-Kunden betroffen gewesen. All-Inkl.com deaktivierte etwa eine Woche nach unserem Hinweis alle DKIM-Signaturen für Mails, die über die PHP-Funktion mail() verschickt wurden.

Private Schlüssel

Bei späteren Untersuchungen bemerkten wir, dass wir teilweise auch per SMTP Mails mit falscher Domain abliefern konnten, die dann signiert wurden – das Problem war bei einigen Anbietern also nicht auf die mail()-Funktion von PHP beschränkt. Die Lücke zeigte wieder ein altbekanntes Problem. DKIM basiert auf asymmetrischer Kryptografie, es gibt also einen öffentlichen und einen privaten Schlüssel. Wirklich sicher sind solche Verfahren nur, wenn der private Schlüssel auch wirklich privat bleibt. Also am besten auf einer Maschine, auf die nur der Inhaber selbst Zugriff hat. Wer DKIM bei einem Shared-Hosting-Dienst nutzt, gewinnt zwar viel Komfort, gibt aber seinen privaten Schlüssel aus der Hand und muss dem Dienstleister vertrauen. (*jam@ct.de*)

[/expand]