Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: INTERNET-DIENSTLEISTER

Sicheres Webhosting

Handlungsempfehlungen für Webhoster

Ungenügend gesicherte Webseiten und Webserver im Internet sind als potenzielle Verbreitungswege für Schadprogramme anzusehen und stellen daher eine Bedrohung dar.

Diese BSI-Empfehlung richtet sich an Webhoster und behandelt Maßnahmen zur Verbesserung der Sicherheit für Webhostingkunden. Hierfür werden die verschiedenen Phasen des Webhostings sowie grundlegende Maßnahmen betrachtet.

Für Maßnahmen zur Konfiguration und den Betrieb von Webanwendungen sei an dieser Stelle zusätzlich auf die Empfehlung „Bereitstellung von Webanwendungen“ hingewiesen.

1 Wahl eines Hostingprodukts und Vertragsabschluss

1.1 Unterstützung des Kunden bei der Wahl eines Hostingprodukts

Am Markt existiert eine Vielzahl unterschiedlicher Produkte, die Kunden von Webhostern offeriert werden. Das Spektrum reicht von Angeboten zur Veröffentlichung einfacher Webseiten bis zur Vermietung von Webservern mit vollständigen Administrationsrechten für Kunden. Aufgrund der Produktvielfalt ist es sinnvoll, die Kunden mithilfe einer prägnanten Produktbeschreibung bei der Auswahl zu unterstützen. So sollte beispielsweise über den Verwaltungsaufwand und die zu übernehmende Verantwortung aufgeklärt werden.

Mit einer ausführlichen und erklärenden Dokumentation ist den Kunden darüber hinaus zu verdeutlichen, welche Verwaltungsbereiche sie im Detail zu verantworten haben sowie welche Funktionen und Einstellungsmöglichkeiten hierbei zur Verfügung stehen. Diese Dokumentation sollte insbesondere auf die jeweiligen Risiken eingehen und Sicherheitsmaßnahmen empfehlen.

1.2 Vertragliche Regelungen mit dem Kunden

Das BSI empfiehlt, vertraglich mit den Kunden zu vereinbaren, dass die Diensteerbringung bei missbräuchlicher Nutzung eingeschränkt bzw. beendet werden kann. Dies kann beispielsweise über eine sogenannte „Acceptable Usage Policy“ geschehen, die Teil des Vertrags mit den Kunden ist.

1.3 Bestellungen mit vorgetäuschten Identitäten (Fake-Bestellungen)

Um Bestellungen mit vorgetäuschten Identitäten und damit oftmals verbundenem Zahlungsbetrug entgegenzuwirken, empfiehlt das BSI Webhostern, sich mit diesem Thema aktiv zu beschäftigen. So könnte eine Maßnahme, wie beispielsweise die zeitweise Einschränkung der initial zur Verfügung gestellten Dienstleistung, in Betracht gezogen werden, um unrechtmäßige Bestellungen unattraktiv zu machen.

2 Produkteinstellungen und Inbetriebnahme

2.1 Basissysteme und Grundeinstellungen

Abhängig von dem durch die Kunden gewählten Hostingprodukt übergibt ein Webhoster einen Teil oder die gesamte Verantwortung für das Betriebssystem und die Basisprogramme an die Kunden. Darunter fallen beispielsweise Basisprogramme, wie Skriptspracheninterpreter und Datenbanksysteme. So erlaubt ein Webhoster seinen Kunden bei einem typischen Shared-Hosting-Produkt z. B. die Auswahl von bestimmten Basisprogrammen und deren Teil-Konfiguration. Die Administration und Wartung des Betriebssystems und der Basisprogramme verbleibt jedoch beim Hoster. Deshalb ist es in diesem Fall wichtig, dass jeder Webhoster den Kunden ein sicheres Basissystem und eine Auswahl von sicher vorkonfigurierten Basisprogrammen zur Verfügung stellt.

Da die den Kunden übergebenen Systeme häufig mit den Grundeinstellungen weiter betrieben werden, ist es bei allen Produkten notwendig, bereits die Basisinstallation sicher zu gestalten. So sollten sowohl das Betriebssystem als auch die zur Verfügung gestellten Basisprogramme auf einem aktuellen Stand sein und ausschließlich Produkte gewählt werden, für die die Verfügbarkeit von Sicherheitsupdates für einen längeren Zeitraum sichergestellt ist. Darüber hinaus sollten alle Komponenten mit als allgemein sicher anerkannten Einstellungen vorkonfiguriert sein. Die durch Hersteller vordefinierten Standard-Konten und -Passwörter sollten bereits vom Hoster durch individuelle Anpassungen abgeändert werden.

Allgemein sollten die Kunden über die Risiken beim Einsatz von zusätzlichen Anwendungen und Erweiterungen (Plug-ins) informiert werden. Darüber hinaus sollten sie regelmäßig auf vorhandene Updates der genutzten Programme hingewiesen werden (z. B. per E-Mail und beim Login in die Verwaltungsoberfläche).

2.2 Information über und Einsatz von sicheren Protokollen

Der Webhoster sollte seinen Kunden die Möglichkeit bieten, sichere Protokolle zu nutzen und diese bereits in den Grundeinstellungen der Hostingprodukte vorsehen. Dies beinhaltet z. B. die sichere Datenübermittlung via SFTP, POP3S, SMTPS und der verschlüsselte Zugriff auf die jeweiligen Administrationsbereiche über HTTPS. Zu allen angebotenen Protokollen sollten angemessene Informationen in der Dokumentation vorhanden sein.

2.3 Produktteile im Verwaltungsbereich der Webhoster

Der Einsatz von Minimalsystemen und sicheren Protokollen sollte für jeden Webhoster selbstverständlich sein. Über die sicheren Grundeinstellungen hinaus sollten zusätzliche Maßnahmen getroffen werden, die die Sicherheit der Betriebssysteme und der angebotenen Dienste erhöhen. Z. B. kann durch den Einsatz von Sandbox-Techniken (chroot-jail und user-mode-linux) und Software die Sicherheitsmodule (z. B. Linux Security Modules) verwenden eine bessere Trennung der einzelnen Kundenbereiche herbeigeführt werden. Weiter können bereits beim Upload von Webinhalten sichere Dateisystemberechtigungen automatisch voreingestellt sowie Inhalte auf Schadprogramme hin überprüft werden.

2.4 Produkte im Verwaltungsbereich des Kunden

Den Kunden, denen die administrativen Rechte eines gesamten Produktes obliegen (meist dediziertes Webhosting), sollten Webhoster Betriebssysteminstallationen anbieten, die auf einem aktuellen und als sicher geltenden Stand sind. Dabei sind auch vorkonfigurierte Installationen für verschiedene Dienste-Server denkbar. So könnten z. B. gehärtete Content Management System (CMS) Server angeboten werden. Darüber hinaus sollten automatische Updates aktiviert werden, falls diese vorgesehen sind.

2.5 Zusatzprogramme

Durch die Nutzung von zusätzlichen Anwendungen, wie frei verfügbaren CMS, ist es den Kunden möglich, auf einfache Weise komplexere Webanwendungen zu realisieren. Dabei sind die meisten dieser Zusatzprogramme wohl bekannt und werden den Kunden oftmals durch den Webhoster zur Installation bereitgestellt.

Das BSI begrüßt eine solche Möglichkeit und empfiehlt hierbei, genau wie bei den Basiskomponenten, eine sichere Vorkonfiguration zu verwenden. Außerdem sollten die jeweiligen Dokumentationen den Kunden leicht zugänglich gemacht werden, z. B. durch Verweise auf geeignete Drittquellen (Herstellerseiten, etc.). Diese Verweise sollten ebenfalls in die eigene Dokumentation aufgenommen werden. Nach Möglichkeit sollten Webhoster darüber hinaus wesentliche Punkte zur Absicherung von Fremdprodukten auch in ihrer Dokumentation aufnehmen sowie für weiterführende Sicherheitsinformationen auf die Webseiten des Bürger-CERT und BSI für Bürger hinweisen.

Optional kann ein Webhoster im Zuge der Bereitstellung solcher Pakete die manuelle Installation des gewählten Zusatzprogramms sowie zusätzlicher Erweiterungen einschränken oder ggf. unterbinden.

3 Systemkontrolle, -pflege und -wartung

3.1 Kontrolle und Pflege von Diensten

Durch die Kunden vorgenommene Änderungen wesentlicher Diensteeinstellungen (insb. sicherheitsrelevanter) sollten z. B. per E-Mail an den jeweiligen Kunden quittiert werden. Ein solches Vorgehen soll Kunden davor bewahren, durch fehlerhafte Konfigurationen ungewollt und unbewusst Dienste bereitzustellen (z. B. Open Resolver) oder Funktionen zu betreiben, die nicht benötigt werden (z. B. Skriptspracheninterpreter). Bei konkreten Hinweisen auf aktiv ausgenutzte Schwachstellen in den verwendeten Diensten der Kunden sollten sich Webhoster mit geeigneten Maßnahmen (z. B. Portsscans) einen Überblick über betroffene Kundensysteme verschaffen und deren Nutzer informieren.

3.2 Produktteile im Verwaltungsbereich von Webhostern

Die Systeme, die durch einen Webhoster administriert werden, sollten vom Webhoster regelmäßig und nach Möglichkeit automatisiert auf Manipulationen, Infektionen und fehlerhafte Konfigurationen hin überprüft werden.

3.3 Produkte im Verwaltungsbereich der Kunden

Durch die einem Kunden zur Verfügung gestellten sicheren Basisinstallationen (siehe „2. Produkteinstellungen und Inbetriebnahme“) ist es einem Webhoster möglich, den Kunden über verfügbare Updates oder notwendige Einstellungsänderungen zu der Installation zu informieren.

3.4 Zusatzprogramme

Bei Zusatzprogrammen, deren Installation ein Webhoster direkt zur Verfügung stellt, sollten Updates zeitnah angeboten werden. Weiter sollten Kunden, die diese Programme nutzen, über evtl. bekannt gewordene Sicherheitslücken informiert werden.

4 Behandlung von technischen Problemen und kompromittierten Kundensystemen

4.1 Kundenbenachrichtigung

Bei vorliegendem Verdacht auf eine Schadprogramm-Infektion, -Verbreitung oder eine missbräuchliche Nutzung des von Kunden genutzten Hostingangebots sollte eine Information an alle Kunden stattfinden. Die Information der Kunden kann per Telefon, Brief oder E-Mail erfolgen.

4.2 Dokumentation und Leitfäden

Neben der oben genannten Dokumentation sollten den Kunden auch Leitfäden bzw. Hilfestellungen zum systematischen Vorgehen bei unterschiedlichen Problemen zur Verfügung stehen. Dies betrifft z. B. die Desinfektion von Webseiten oder die Wiederherstellung eines Webservers. Hierbei ist auch denkbar, die Kunden im Zuge der Kundenbenachrichtigung mit einer zum Problem passenden, technisch detaillierten Hilfestellung zu unterstützen.

4.3 Unterstützung von Kunden bei einem kompromittierten System

Im Falle einer Schadprogramm-Infektion, -Verbreitung oder einer missbräuchlichen Nutzung des von Kunden genutzten Hostingangebots sollte der Webhoster die Kunden bei der Bereinigung bzw. der Absicherung des Systems unterstützen. Dies betrifft auch Systeme, deren Zugangsdaten in die Hände unbefugter gelangt sind (z. B. über Phishing).

Die Unterstützung der Kunden geht über die reine Bereitstellung von Leitfäden (siehe Dokumentation und Anleitungen) hinaus. Sie beinhaltet ein zeitnahes Tätigwerden, um eine Schadprogramm-Infektion, -Verbreitung oder eine missbräuchliche Nutzung zu bereinigen oder den Zugang zu ihr zu sperren, sobald ein Webhoster hiervon Kenntnis erlangt.

5 Grundlegende technische und organisatorische Maßnahmen

5.1 Weiterverkäufe(r) (Reseller)

Webhoster sollten die Möglichkeiten für Weiterverkäufe von Webhostingprodukten oder Teilprodukten durch Kunden klar regeln. Sollten Weiterverkäufe nicht vorgesehen sein, ist dies vertraglich festzuhalten. Wenn Weiterverkäufe jedoch ermöglicht werden sollen, so sollten Webhoster ihren Kunden bewusst machen und auch vertraglich festhalten, dass diese die Verantwortung für ihre eigenen Vertragspartner gegenüber dem Webhoster übernehmen. Daher sollte den Kunden, die als Weiterverkäufer agieren möchten, ebenfalls empfohlen werden, die hier genannten Empfehlungen nach Möglichkeit ebenso umzusetzen.

5.2 Bildung eines Abuse-Teams

Es ist für Webhoster empfehlenswert, innerhalb ihres Unternehmens eine organisatorische Einheit zu schaffen, die sich um die Abwendung von Sicherheitsvorfällen in der eigenen Infrastruktur und auf den Kunden-Systemen kümmert und Maßnahmen bei eingetretenen Sicherheitsvorfällen ergreift. Durch ein Abuse-Team sollte sichergestellt werden, dass unabhängig von der IT-System-Administration präventive Maßnahmen (Bugtracker, etc.) umgesetzt und eingetretene Sicherheitsvorfälle dediziert behandelt werden. Zur Verbesserung der Reaktionszeiten sowie zur Entlastung der Mitarbeiter von Routinetätigkeiten sollten Systeme zum Einsatz kommen, die eintreffende Vorfallsmeldungen automatisiert vorfiltern und verarbeiten können. Diese sollten die international etablierten Verfahren und Protokolle zum Austausch von Vorfallsmeldungen, wie beispielsweise X-ARF (Extended Abuse Reporting), implementieren.

5.3 IT-Sicherheitskonzept

Es ist wichtig, die Infrastruktur mithilfe eines IT-Sicherheitskonzeptes zu planen und zu dokumentieren. Hierbei spielen insbesondere die Verantwortlichkeiten, die Zugriffsrechte, die Einsatzzwecke und die bei Vorfällen notwendigen Gegenmaßnahmen eine zentrale Rolle.

5.4 Schutzmaßnahmen in der Infrastruktur

Grundsätzlich sollten die Kundensysteme vom Firmennetzwerk des Webhosters getrennt in einem separaten Netzwerk verwaltet werden. Dabei sollten auch Schutzmaßnahmen getroffen werden, um zu verhindern, dass Kundensysteme auf das interne Netzwerk des Webhosters oder auch andere Kundensysteme zugreifen können.

Zusätzlich zu den gängigen Schutzmaßnahmen, die in Infrastrukturen genutzt werden (z. B. Firewalls), ist die Nutzung von weiteren Systemen, die mögliche Angriffe identifizieren können, bei Webhostern zu empfehlen. Dies betrifft beispielsweise Honeypots, Spamtraps, Web-Crawler und Intrusion-Detection-Systeme.

Zur Sicherung der eigenen Infrastruktur könnten darüber hinaus auch Systeme eingesetzt werden, die es ermöglichen, unsicher konfigurierte Systeme im eigenen Netz zu erkennen. Hier wären z. B. Integritätsüberprüfungen von virtuellen Maschinen oder ein Network-Access-Control-Verfahren bzgl. ungepatchter Systeme denkbar.

Weiterhin sollten die Informationsquellen existierender Botnetz-Meldedienste (beispielsweise Shadow Server) genutzt werden, um Hinweise auf infizierte Systeme eigener Kunden zu erhalten. Gehostete Webseiten sollten regelmäßig auf Infektionen bzw. Bereitstellung von infizierten Dateien überprüft werden oder externe Dienstleistungen, wie z. B. Google-Safebrowsing, diesbezüglich in Anspruch genommen werden.

Weiterführende Empfehlungen zur sicheren Konzeption von Netzwerken und Serversystemen finden Sie in der ISi-Reihe (z. B. ISi-Web, ISi-Lana und ISi-Mail) und den IT-Grundschutz-Katalogen des BSI.

5.5 Logdaten

Art und Umfang der Protokollierung von Nutzungsdaten und Verkehrsdaten sollten in Abstimmung mit dem zuständigen Datenschutzbeauftragten klar festgelegt sein. Dies umfasst die Festlegung auf definierte Logverfahren, Aussagen zur Speicherdauer protokollierter Daten sowie der Art der Protokollierung. Aus Sicherheitsgründen ist eine Protokollierung in jedem Fall notwendig, um Angriffe frühzeitig erkennen und nachvollziehen zu können. Nur so ist gewährleistet, dass die richtigen Gegenmaßnahmen ergriffen werden.

6 Unternehmensübergreifende Kooperation

6.1 Zusammenarbeit mit anderen Webhostern

Webhoster – und dabei insbesondere die jeweiligen Abuse-Teams – sollten Informationen über infizierte Webseiten/Webserver untereinander austauschen. Eingehende Meldungen sollten (ggf. automatisiert) zentral und zeitnah bearbeitet werden. Webhoster sollten aktiv mit dem BSI zusammenarbeiten, mit dem Ziel, Gefährdungen für Bürger im Internet zu vermeiden.

6.2 Zusammenarbeit mit AV-Herstellern

Vorliegende Schadprogramme sollten zeitnah an AV-Hersteller weitergeleitet werden, um diese bei der Entwicklung von Schutzmaßnahmen zu unterstützen.

Diese BSI-Empfehlung ist unter Mitwirkung der als Partner der Allianz für Cyber-Sicherheit registrierten Internet-Service-Provider 1&1 Internet AG, Deutsche Telekom und Vodafone sowie den Internetdienstleistern Strato AG und Hetzner Online AG entstanden.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.