



EMPFEHLUNG: INTERNET-DIENSTLEISTER

Malware-Schutz

Handlungsempfehlungen für Internet-Service-Provider (ISP)

Der Themenkomplex „Malware“ stellt aktuell eine der größten Bedrohungen für Internet-Nutzer dar. Diese BSI-Veröffentlichung zur Cyber-Sicherheit behandelt Maßnahmen zum Malware-Schutz, die durch Provider im Privatkundenbereich umgesetzt werden sollten. Die Empfehlungen umfassen die Bereiche Kundenunterstützung (Customer-Support), technische Schutzmaßnahmen sowie providerübergreifende Kooperation.

1 Kundenunterstützung

1.1 Sensibilisierung

Neukunden von ISPs erhalten Unterlagen mit Konfigurationsdaten und Informationsmaterial üblicherweise per Post. Das BSI empfiehlt, Neukunden auf diesem Weg auch mit Informationen zu Risiken im Internet, bestehenden Schutzmöglichkeiten sowie Hinweisen zu Entfernungsmöglichkeiten von Schadsoftware, zu versorgen.

1.2 Kundenbenachrichtigung

Bei vorliegendem Verdacht auf eine Schadsoftware-Infektion eines Kunden-Endgeräts sollte der Kunde benachrichtigt werden. Die Information kann per Brief, E-Mail oder über eine Vorschaltseite / Walled-Garden Lösung (als Informationskanal) erfolgen.

1.3 Information über Schutzmaßnahmen

Kunden sollten in geeigneter Form auf zu ergreifende Schutzmaßnahmen bei den von ihnen verwendeten Endgeräten aufmerksam gemacht werden. Das BSI hat Empfehlungen sowohl für den Betrieb von PCs unter Microsoft Windows („Sichere Nutzung von PCs unter Microsoft Windows – Empfehlungen für Privatanwender“), den Betrieb von Macs unter OS X („Sichere Nutzung von Macs unter Apple OS X Mountain Lion“) sowie die Nutzung von PCs unter Ubuntu („Sichere Nutzung von PCs unter Ubuntu“) veröffentlicht. In Verbindung mit dem Betrieb von PCs unter Microsoft Windows sollten Hinweise auf kommerzielle und freie Anti-Virus-Produkte gegeben werden oder auch eine optionale Bereitstellung eines AV-Produkts als Bundle zusammen mit dem Internetanschluss erfolgen.

1.4 Unterstützung von Endkunden bei der Entfernung von Schadsoftware

Provider sollten ihren Kunden Unterstützung bei der Entfernung von Schadsoftware anbieten. Dies kann beispielsweise über die Teilnahme des Providers am Anti-Botnet-Beratungszentrum ABBZ (s. u.) erfolgen.

1.5 Vertragliche Regelungen mit den Kunden

Das BSI empfiehlt, vertraglich (zum Beispiel in den AGB) mit den Kunden zu vereinbaren, dass die Dienstleistung bei missbräuchlicher Nutzung eingeschränkt werden kann. Dies kann beispielsweise über eine sogenannte „Acceptable Use Policy“ geschehen, die Teil des Vertrags mit dem Kunden ist.

2 Zusammenarbeit mit Hardware-Herstellern

In Zusammenarbeit mit den Herstellern von (IAD-)Routern, die typischerweise von Endkunden zur Internetnutzung eingesetzt werden, sollten

- a) sinnvolle Schutzfunktionen entwickelt und
- b) sichere Voreinstellungen vereinbart werden,

die den Kunden optimal vor dem Befall von Schadsoftware sowie dem Missbrauch seines Internetanschlusses schützen.

3 Zusammenarbeit mit AV-Herstellern / Anti-Botnet-Beratungszentrum (ABBZ)

3.1 Zusammenarbeit mit AV-Herstellern

Mithilfe der umgehenden Weiterleitung von Malware-Samples an AV-Hersteller können diese bei der zeitnahen Entwicklung von Schutzmaßnahmen unterstützt werden.

3.2 Anti-Botnet-Beratungszentrum

Im Jahr 2011 hat das Anti-Botnet-Beratungszentrum (ABBZ) seinen Betrieb aufgenommen. Das ABBZ gibt Endkunden Hilfestellung im Fall einer Schadsoftware-Infektion und stellt Anti-Bot-CDs zur Verfügung. Teilnehmende Provider tauschen Informationen über infizierte Endgeräte untereinander aus und informieren eigene Kunden bei Infektionsverdacht. Das BSI empfiehlt die Teilnahme am Anti-Botnet-Beratungszentrum. Weitere Informationen erhalten Sie unter www.botfrei.de.

4 Providerübergreifende Kooperation

Bei der Entwicklung von Sicherheitsmaßnahmen ist der providerübergreifende Austausch zu infizierten Geräten sehr hilfreich. Es sollte ein funktionierender Abuse-Kontakt eingerichtet sein, über den eingehende Meldungen (ggf. automatisiert) bearbeitet werden. Bei providerübergreifenden Störungen (z. B. DDoS-Angriff) sollte eine gegenseitige Hilfestellung erfolgen. Provider sind dazu aufgerufen, aktiv mit dem BSI zusammenzuarbeiten, um Gefährdungen für Bürger im Internet zu vermeiden.

5 Technische Maßnahmen

5.1 Schutzmaßnahmen auf dem Mailserver

ISPs sollten auf eigenen Mailservern eine Viren- sowie Spamprüfung bei sämtlichen eingehenden und ausgehenden Mails vornehmen. Die Prüfung sollte auch Attachments und Inhalte von gepackten Attachments einschließen.

5.2 Temporäre Verbindungssperre

Bei Missbrauch des Internetanschlusses für den Spam-Versand bzw. bestehendem Verdacht auf Schadsoftware-Infektion, ist die Einrichtung einer vorübergehenden, verdachtsabhängigen, abgehenden Verbindungssperre zu externen Mailservern (Sperrung des Ports 25) ein zweckdienliches Instrument. Auf diese Weise werden die Auswirkungen für Dritte wirkungsvoll reduziert. Der Kunde sollte bei Durchführung einer solchen Maßnahme umgehend informiert werden und die Möglichkeit erhalten, eine Aufhebung der Sperrung selbst zu veranlassen.

5.3 Anti-IP-Spoofing Maßnahmen

Um Angriffen, bei denen gespooft IP-Adressen zum Einsatz kommen, entgegenzuwirken, sollten an den Netzübergängen in andere Providernetze die Maßnahmen gemäß BCP38¹ umgesetzt sein.

5.4 Logdaten

Die Protokollierung von Nutzungsdaten und Verkehrsdaten sollte in Abstimmung mit dem Datenschutzbeauftragten klar festgelegt sein. Dies umfasst die Festlegung definierter Logverfahren, Aussagen zur Speicherdauer protokollierter Daten sowie der Art der Protokollierung.

5.5 Schadsoftware-Detektion

Um Missbrauch einzudämmen, können geeignete Detektionsverfahren (beispielsweise Honey-pots, Spamtraps oder Web-Crawler) zur Erkennung infizierter Systeme eingesetzt werden. Die gewonnenen Erkenntnisse sollten mit anderen Providern ausgetauscht werden (s. o.).

Weiterhin ist die Nutzung der Informationsquellen existierender Botnetz-Meldedienste (beispielsweise Shadow Server) zu empfehlen, um Hinweise auf infizierte Systeme eigener Kunden zu erhalten.

Gehostete Webseiten sollten regelmäßig auf Infektionen bzw. Bereitstellung von Drive-by-Exploits überprüft werden.

Bei diesen Maßnahmen sind die rechtlichen Vorgaben, insbesondere des Datenschutzrechts und des Fernmeldegeheimnisses, einzuhalten.

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 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.

1 <http://tools.ietf.org/html/bcp38>