

Weitere Informationen: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Flyer-IT-Sicherheitspreis-Horst-Goertz-2014.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Flyer-IT-Sicherheitspreis-Horst-Goertz-2014.pdf?__blob=publicationFile)

## BSI veröffentlicht Mindeststandard für verschlüsselte Internetverbindungen

Im Rahmen der IT-Fachmesse it-sa in Nürnberg hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) am 08.10.2013 einen Mindeststandard für den Einsatz einer Transportverschlüsselung mittels des TLS-Protokolls veröffentlicht. Demnach wird in der Bundesverwaltung das Protokoll TLS 1.2 in Kombination mit Perfect Forward Secrecy (PFS) als Mindeststandard auf beiden Seiten der Kommunikationsbeziehung vorgegeben. Zudem muss dies durch eine geeignete, dem Schutzbedarf entsprechende, Konfiguration ergänzt werden. Der Mindeststandard kann neben Einrichtungen der Bundesverwaltung auch Unternehmen, Webseitenbetreiber und andere Institutionen dabei unterstützen, das eigene IT-Sicherheitsniveau sowie das ihrer Kunden und Partner zu erhöhen. Dabei ist der Mindeststandard als Handlungsempfehlung zu verstehen, um sicher über das Internet kommunizieren zu können. Das BSI empfiehlt Anwendern aufgrund der dynamischen IT-Bedrohungslage einen raschen und möglichst flächendeckenden Umstieg auf TLS 1.2.

Das TLS-Protokoll (Transport Layer Security) dient der Sicherstellung von Vertraulichkeit, Authentizität und Integrität bei der Übertragung von Daten in unsicheren Netzwerken. So kommt die TLS-gesicherte Übertragung im Internet (mittels HTTPS) bei zahlreichen Anwendungen wie Homebanking, eCommerce oder eGovernment zum Einsatz und soll gewährleisten, dass sensible Informationen wie Zugangsdaten, PINs oder Passwörter sicher übertragen werden können.

### Vom Mindeststandard zur Verwaltungsvorschrift

Gemäß § 8 Absatz 1 des BSI-Gesetzes hat das BSI die Befugnis, allgemeine technische Mindeststandards für die Sicherung der Informationstechnik des Bundes festzulegen. Der Mindeststandard beschreibt die zu erfüllenden sicherheitstechnischen Anforderungen an eine Produkt- bzw. Dienstleistungskategorie oder Methoden, um einen angemessenen Mindestschutz gegen IT-Sicherheitsbedrohungen zu erreichen. Mindeststandards stellen zunächst unverbindliche Empfehlungen dar. Nach Zustimmung des IT-Rats kann das Bundesministerium des Innern die im Mindeststandard formulierten Anforderungen ganz oder teilweise als allgemeine Verwaltungsvorschrift erlassen und dadurch für die Bundesverwaltung für verbindlich erklären. Darüber hinaus kann auch der IT-Planungsrat die Mindeststandards des BSI als gemeinsame Standards für den Datenaustausch zwischen Bund und den Ländern festlegen.

### Schutzbedarf individuell analysieren

Eine Migration zu TLS 1.2 umfasst in der Regel nicht nur Software-, sondern auch Hardware-Produkte und kann kosten- und zeitintensiv sein. Daher rät das BSI, bis zur Umstellung zusätzliche Schutzmaßnahmen umzusetzen. So kann TLS 1.0 in bestehenden Anwendungen übergangsweise weiter eingesetzt werden, sofern geeignete Schutzmaßnahmen gegen bereits bekannte Angriffe gegen das SSL/TLS-Protokoll (z. B. BEAST, CRIME) ergriffen werden. Zudem sollten während der Übergangsphase alternative Maßnahmen zum Schutz der Vertraulichkeit der Kommunikation getroffen werden.

So sollte sich beispielsweise der TLS-Server in einer gesicherten Umgebung befinden, damit kein Angreifer Zugriff auf den geheimen Schlüssel erlangen kann.

Hier steht das Dokument zum Download bereit: [https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard\\_BSI\\_TLS\\_1\\_2\\_Version\\_1\\_0.pdf?\\_\\_blob=publicationFile](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf?__blob=publicationFile)

## BSI-Studie: Notfallmanagement mit der Cloud für KMU

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 08.10.2013 eine Studie zum Thema „Notfallmanagement mit der Cloud für KMU“ veröffentlicht. Die Studie beleuchtet Potenziale von Cloud-Techniken für die Absicherung eines Ausfalls IT-gestützter Geschäftsprozesse in kleinen und mittleren Unternehmen (KMU). Ziel der Studie ist es, praxisnahe Methoden zur Notfallprävention und -reaktion aufzuzeigen, die mithilfe moderner Virtualisierungs- und Cloud-Technologien umgesetzt werden können. Im Fokus steht dabei eine Betrachtung der auf dem Markt verfügbaren Cloud-Angebote für das Notfallmanagement von KMU sowie deren Einsatz in drei typischen Szenarien. Die Studie zeigt, dass der Einsatz von Cloud-Techniken das Notfallmanagement sowie verschiedene Kontinuitätsstrategien von Unternehmen verbessern können.

Kleine und mittlere Unternehmen stehen in der Regel unter hohem Kostendruck und haben daher selten Ressourcen für ein umfassendes Notfallmanagement. Aus dem gleichen Grund setzen viele KMU bereits Virtualisierungstechniken ein. Die Studie verdeutlicht, dass in KMU durch den Einsatz dieser Virtualisierungstechniken sowie von Cloud-Diensten fast automatisch eine höhere Verfügbarkeit und Ausfallsicherheit der IT-gestützten Geschäftsprozesse erreicht wird.

Bisherige Ansätze zur Absicherung eines Ausfalls der Geschäftsprozesse beinhalten, die entsprechende Hardware doppelt vorzuhalten bzw. diese nach einem Notfall gegebenenfalls neu zu beschaffen. Beides ist in der Regel mit nennenswerten finanziellen und zeitlichen Aufwänden verbunden. Mit der Nutzung von Virtualisierungs- und Cloud-Techniken können diese Aufwände deutlich reduziert werden. Damit sind Cloud-Techniken ein Innovationstreiber beim Notfallmanagement.

„Die Studie zeigt, dass Cloud-Technologien gerade für KMU konkrete Anwendungsszenarien bieten, mit denen die Unternehmen ein Stück mehr Informationssicherheit schaffen können. Vertrauen in die Sicherheit der Cloud ist dabei eine wichtige Voraussetzung. Dieses Vertrauen zu schaffen, ist eine zentrale Aufgabe der Cloud-Dienstleister, wenn sie eine dauerhafte Akzeptanz von Cloud-Diensten erreichen wollen. Auch das BSI als Nationale IT- und Cyber-Sicherheitsbehörde trägt hier seinen Teil bei, indem wir uns bereits seit einigen Jahren intensiv der Frage nach der Sicherheit von Cloud-Angeboten und der Schaffung von entsprechenden Standards widmen“, erklärt Michael Hange, Präsident des BSI.

Mit der Durchführung der Studie hatte das BSI die HiSolutions AG beauftragt. Die Studie ist auf der Webseite des BSI kostenlos zum Download verfügbar. [https://www.bsi.bund.de/DE/Themen/Cloud-Computing/Studien/Studien\\_node.html](https://www.bsi.bund.de/DE/Themen/Cloud-Computing/Studien/Studien_node.html)