Software-Erweiterung für Outlook 2010 zur Signatur und Verschlüsselung von E-Mails „versteht“ jetzt alle Sprachen

Ob arabisch, hebräisch, japanisch, chinesisch oder russisch – mit der neuen Version 2.1 von *gpg4o* für Outlook 2010 können jetzt auch Mails mit den Schriftzeichen dieser und anderer Sprachen zuverlässig und fehlerfrei verarbeitet und geschützt werden. Die Verschlüsselungs- und Signatur-Software des IT-Systemhauses Giegerich & Partner kann 45 Tage lang kostenlos getestet werden.

Dreieich, 21.06.2012 – Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt zu Recht: „*Eine E-Mail gleicht nicht etwa einem Brief, sondern vielmehr einer Postkarte: Alles, was darauf steht, ist für jeden zu lesen, der die Karte weiter zum Empfänger transportiert*“.
Das IT-Systemhaus Giegerich & Partner hat mit *gpg4o* eine Software-Erweiterung für Outlook 2010 ® zur Verschlüsselung und digitalen Signatur von E-Mails entwickelt, die auf dem OpenPGP-Standard basiert und eine wichtige Funktionslücke in diesem weit verbreiteten Kommunikationsprogramm von Microsoft schließt.
“*Mit der neuen, verbesserten Version 2.1 des in deutsch und englisch verfügbaren Add-Ins können jetzt Mails aller Sprachen der Welt zuverlässig und fehlerfrei verarbeitet werden – also auch im arabischen, hebräischen, japanischen, chinesischen oder kyrillischen Alphabet oder mit sonstigen ‚exotischen’ Schriftzeichen*”. erläutert Geschäftsführer Hans-Joachim Giegerich. Neben der Internationalisierung (durch vollständige UTF-8 Integration) wurden bei der Version 2.1 noch folgende Funktionen optimiert:

- einfache Integration im Terminalserver-Betrieb
- verbesserte Unterstützung von PGP/MIME E-Mails
- erweiterte Interoperabilität mit anderen Verschlüsselungssystemen auf OpenPGP-Basis
- viele kleine funktionale Verbesserungen – basierend auf Kunden-Feedback

Das Add-In kann leicht in Outlook 2010 integriert werden und fügt sich nahtlos in die Software-Oberfläche ein. Die Bedienung ist sehr einfach:

Signierte und/oder verschlüsselte E-Mails werden für den Anwender leicht erkennbar angezeigt. Dabei signalisiert ein Schloss die Verschlüsselung, während das Siegel-Symbol auf eine digitale Signatur hinweist.

Der Empfänger kann sich außerdem detaillierte Informationen darüber anzeigen lassen, wer die digitale Signatur erzeugt hat (um festzustellen, ob die Signatur zur angegebenen E-Mail-Adresse des Absenders passt) oder mit welchen Algorithmen die elektronische Nachricht verschlüsselt wurde. Die Kryptographie- und Signatur-Software ver- und entschlüsselt auch automatisch die per Mail gesendeten Datei-Anhänge (Attachments) mit und ist kompatibel mit allen gängigen Verschlüsselungsprogrammen (z.B. PGP Desktop, Enigmail, etc.).

gpg4o 2.1 läuft auf allen Microsoft-Betriebssystemen ab Windows XP (Service-Pack 3) und benötigt nur Outlook 2010 (idealerweise in einer Microsoft Exchange-Umgebung) sowie die freie Software GnuPG (Version 1.4.2 bis einschließlich 2.0).
Eine detaillierte und verständliche Funktionsbeschreibung der Software-Erweiterung inklusive Kompatibilitätsinformationen sowie eine kostenlose, 45 Tage gültige Testversion ist unter http://www.gpg4o.de abrufbar. Die Vollversion ist im online-Shop unter https://shop.giepa.de erhältlich. Der Preis beginnt bei 93,99 Euro für eine Einzellizenz und ist gestaffelt nach der Anzahl der Lizenzen. Optionale Support-Verlängerungen von ein bis fünf Jahren können gegen einen geringen Aufpreis auch gleich online mit bestellt werden.

Hintergrundinformation 1:

Unverschlüsselte Mails werden in lesbarem Klartext übertragen

Wenn eine E-Mail versendet wird, werden die Datenpakete der E-Mail vom eigenen Mailserver (des Providers) an den Ziel-Mailserver des Empfängers gesendet. Dabei passiert die E-Mail meistens mehrere Knoten im Internet, bis sie am Zielserver ankommt. Der Mailserver des Empfängers überträgt schließlich die E-

Mail auf den Rechner des Empfängers. Während des ganzen Transportweges werden die Datenpakete stets in lesbarem Klartext übertragen. Das heißt, an verschiedenen Stationen des Weges kann die E-Mail mitgelesen und auch verändert werden: Auf dem Weg vom eigenen Rechner zum Mailserver, zwischen den einzelnen Rechnern während des Transportes und vom Ziel-Mailserver zum Empfänger. Verschafft sich eine Person einen illegalen Zugang zu einem der beteiligten Rechner und Internetknoten, kann auch dort direkt die E-Mail abgefangen werden. Zu diesem Zweck gibt es spezielle Programme wie die „Paket-Sniffer", mit denen Datenpakete abgefangen werden können. Die abgefangenen Pakete können auch in ihrem Inhalt verändert und wieder in den Datenstrom eingespeist werden.
Zusätzlich können Geheimdienste und Polizeibehörden aufgrund gesetzlicher Befugnisse und mit richterlicher Erlaubnis E-Mails von dem Provider, der den Mailaccount zur Verfügung stellt, zu Überwachungszwecken anfordern.

50 Prozent der Unternehmen verschicken noch ungeschützte Mails

„*In 50 Prozent der Unternehmen werden E-Mails während der Übertragung durch keinerlei Maßnahme vor unberechtigter Einsichtnahme, Missbrauch oder Manipulation geschützt*", warnte der Verein Deutschland sicher im Netz e.V. (www.sicher-im-netz.de) schon im Jahr 2011. Diese eklatanten Versäumnisse beim E-Mail-Schutz können Sender und Empfänger teuer zu stehen kommen – etwa wenn dadurch vertrauliche bzw. sensible Daten in falsche Hände gelangen (Stichwort: Industrie- bzw. Wirtschaftsspionage!). Dabei kann schon mit relativ geringem Aufwand die Vertraulichkeit von Informationen durch Verschlüsselung garantiert werden, während mit digitalen Signaturen sichergestellt wird, dass eine Datei bzw. eine Nachricht authentisch und unverfälscht ist – also nicht manipuliert wurde.

Hintergrundinformation 2:

- Bericht des online-Portal ‚*searchsecurity.de'* zur **Produkteinführung von *gpg4o:*** http://www.searchsecurity.de/themenbereiche/applikationssicherheit/e-mail-sicherheit/articles/332951
- **GnuPG (GNU Privacy Guard) – Open Source Verschlüsselung aus Deutschland**
  GnuPG ist wie PGP (Pretty Good Privacy) ein Verschlüsselungsprogramm, das die Spezifikationen für Pretty Good Privacy (OpenPGP) nach RFC 4880 des Internet Standardisierungsgremiums IETF (Internet Engineering Task Force) implementiert.

⇨ ⇨

Weiterführende Informationen:

- zu GnuPG (GNU Privacy Guard) / GPG: http://de.wikipedia.org/wiki/GNU_Privacy_Guard
- zu OpenPGP: http://de.wikipedia.org/wiki/OpenPGP

Unternehmensinformationen:

Giegerich & Partner GmbH

Der IT-Dienstleister Giegerich & Partner GmbH mit Sitz in Dreieich bei Frankfurt/M. hat sich auf Lösungen für den reibungslosen und sicheren Betrieb von Netzwerken und computergesteuerten Anwendungen spezialisiert. Neben der Beratung und Konzeption übernimmt Giegerich & Partner die komplette Ausführungen von IT-Projekten sowie den Betrieb von IT-Systemen und -Lösungen im Outsourcing. Kundenspezifische Individuallösungen und die „Veredelung“ bzw. Anpassung von IT-Standardprodukten an die Bedürfnisse von Unternehmen gehört zu den Stärken des IT-Spezialisten. Weitere Informationen unter: http://www.giepa.de

Pressekontakt:

Giegerich & Partner GmbH
Hans-Joachim Giegerich
Robert-Bosch-Str. 18

63303 Dreieich

Tel.: +49-(0)6103-5881-0
Fax.: +49-(0)6103-5881-39

E-Mail: info@giepa.de
www.giepa.de

Redaktionsbüro Spierling
Detlev Spierling
St. Hedwigsweg 1
61440 Oberursel/Ts.

Tel.: +49-(0)700-80008002
Fax.: +49-(0)6171-86 66 55 6

Mobil-Tel.: +49-(0)172-66 46 0 46
E-Mail: presse@spierling.de