Sichere E-Mails Dank verbesserter Signatur- und Verschlüsselungssoftware für Outlook 2010

Mit der Outlook-Erweiterung *gpg4o* können Unternehmen ihre E-Mail-Kommunikation jetzt auch nach dem freien Kryptographiesystem GnuPG zuverlässig absichern. Die verbesserte Version 2.0 der leistungsfähigen Verschlüsselungssoftware ist ab sofort im online-Shop des IT-Systemhauses Giegerich & Partner erhältlich.

Dreieich, 05.03.2012 – „*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 letzten Jahr. 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. 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.

gpg4o schließt eine wichtige Funktionalitätslücke in Outlook 2010

Mit *gpg4o* hat das IT-Systemhaus Giegerich & Partner eine Erweiterung für Outlook 2010 zur Verschlüsselung und digitalen Signatur von E-Mails entwickelt, die eine bis dato bestehende Funktionalitätslücke in diesem beliebten und weit verbreiteten Kommunikationsprogramm von Microsoft schließt. Die neue verbesserte Version 2.0 des auf dem OpenPGP-Standard basierenden Add-Ins ist jetzt über den online-Shop unter https://shop.giepa.de erhältlich.

Das Add-In kann leicht in Outlook 2010 integriert werden. 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.).
"*Das sehr anwenderfreundlich gestaltete gpg4o 2.0 passt sich nahtlos in die Outlook-Oberfläche ein und wurde von uns in einigen wesentlichen funktionalen Details noch weiter entwickelt*", erläutert Geschäftsführer Hans-Joachim Giegerich. Die neue Version enthält folgende Produktverbesserungen:

- Empfang/Versand von Mails um HTML-Format
- Empfang von PGP/MIME-Mails
- Unterstützung von GnuPG 2.0 (GNU Privacy Guard / GPG)
- automatische Netzwerk-Installationsroutine ('Silent Installation')
- automatische Installation von Updates
- Erhöhte Kompatibilität mit anderen Verschlüsselungsprodukten
- Erhöhte Kompatibilität mit anderen Mail-Servern
- optimierte Benutzerführung

gpg4o 2.0 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 (an Version 1.4.2 bis einschließlich 2.0).
Eine detaillierte und verständliche Funktionsbeschreibung der Software-Erweiterung inklusive Kompatibilitätsinformationen ist unter www.gpg4o.de abrufbar.
Der Preis beginnt bei 93,99 Euro für eine Einzellizenz und ist gestaffelt nach Anzahl der Lizenzen. Optionale Support-Verlängerungen von ein bis fünf Jahren können gegen einen geringen Aufpreis auch gleich online mit bestellt werden.

Hintergrundinformationen:

- zur **Produkteinführung von *gpg4o*** (Bericht des online-Portal *‚searchsecurity.de'*): http://www.searchsecurity.de/themenbereiche/applikationssicherheit/e-mail-sicherheit/articles/332951

- zum Thema **E-Mail-Übertragung und –Überwachung**

Wenn eine E-Mail versendet wird, werden die Datenpakete der E-Mail zum Mailserver des Providers übertragen, von wo sie an den Ziel-Mailserver des Empfängers gesendet werden. Dabei passiert die E-Mail meistens mehrere Rechner 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 abgefangen 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, 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.

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.

GnuPG bedient sich dazu wie PGP eines hybriden Verschlüsselungsverfahrens, das aus der Weitergabe eines öffentlichen Schlüssels zur Verschlüsselung und eines privaten Schlüssels zur Entschlüsselung besteht. Zur Verschlüsselung wird eine ganze Reihe symmetrischer Kryptoalgorithmen mit zwei asymmetrischen Public-Key Kryptoalgorithmen kombiniert.

Neben der Nachrichtenverschlüsselung wird GnuPG auch zur Verschlüsselung von Dateien verwendet, die zum Beispiel lokal auf der eigenen Festplatte gespeichert sind. (Quelle: https://hp.kairaven.de/pgp/gpg/gpg1.html)

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
125 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