



Output
09/2008



SECURITY FLASH

Vertrauensverluste

Was haben CNN Top Ten News, UPS und FedEx Paket-Statusmails, MSCN Breaking News und MidWest Airlines-Sonderangebote gemeinsam? – Eine Reihe von professionellen Virenattacken alleine am vergangenen Wochenende.

Was ursprünglich mit der Neugier der Leute und Attacken im Consumer-Bereich begann, verlagert sich nun immer mehr auf vermeintliche Nachrichten seriöser Unternehmen. Sehr beliebt im Moment das Verwirrspiel mit UPS-Statusmails:

"Unfortunately we were not able to deliver postal package you sent on August the 18th in time because the recipient's address is not correct.

*Please print out the invoice copy attached and collect the package at our office
Your UPS"*

Unschwer auszurechnen, dass solche Mails vor allem im Geschäftsbereich, wo UPS für Kurier-Dienste verwendet wird, gute Chancen auf erfolgreiche Infektion haben. Dabei sind diese Attacken selbst für Spezialisten kaum als solche zu erkennen. Täuschend echt sehen die nachgemachten HTML-Mails aus – nur dass ein Doppelklick auf das vermeintliche PDF im Attachment oder ein Klick auf den beigefügten Link völlig ausreicht, um einen Erstinfiltrator auf das Zielsystem zu bringen – der kann dann je nach Angriffsentention beliebig weitere Module nachladen oder weiterführende Informationen evaluieren. Dabei stehen wir erst am Anfang einer verhängnisvollen Entwicklung. Wenn potenzielle Angreifer weiter erkennen, dass Sie im Bereich von Newslettern, Statusmeldungen oder sonstigen »erwarteten« oder für den Geschäftsprozess notwendigen Inhalten aufsetzen können, haben sie nicht nur eine weitere effektive Methode gefunden Systeme zu infizieren, sondern eine nachhaltig weitaus kritischere Entwicklung angestoßen: Sie erodieren das Vertrauen in die Herkunft von Daten aus vermeintlich seriösen Quellen. Eine korrekte Einschätzung möglicher Bedrohungen wird für Anwender immer schwieriger.

Josef Pichlmayr
Geschäftsführer von IKARUS Software
www.ikarus.at
www.mymailwall.com