

**26. INTERNATIONALE KONFERENZ FÜR DEN SCHUTZ DER PRIVATSPHÄRE
UND DEN DATENSCHUTZ
WROCLAW, 14.-16. SEPTEMBER 2004**

**Die Änderungen der EntschlieÙung von der Konferenz 2003
zur Automatischen Software-Aktualisierung**

EntschlieÙung

Auf Vorschlag des Australischen Bundesbeauftragten für den Schutz der Privatsphäre, des Beauftragten für die Information und die Privatsphäre von Ontario, des Datenschutzbeauftragten von Hongkong und des Beauftragten für den Datenschutz und den Zugang zur Information von Brandenburg nimmt die Internationale Konferenz folgende EntschlieÙung an:

1. Die Konferenz stellt mit Besorgnis fest, dass Software-Unternehmen weltweit immer häufiger nicht-transparente Techniken benutzen, um die Software-Aktualisierungen auf die Computer der Nutzer zu übertragen.

Dadurch sind sie in der Lage:

- die personenbezogenen Daten, die auf dem Computer des Nutzers gespeichert sind (z. B. Browser-Einstellungen oder Informationen über das Nutzungsverhalten) auszulesen und zu sammeln, ohne dass der Nutzer dies bemerken, beeinflussen oder verhindern kann,
- zumindest die teilweise Kontrolle über den Zielcomputer zu gewinnen und damit die Möglichkeit des Nutzers einzuschränken, seinen rechtlichen Verpflichtungen zur Gewährleistung der Datensicherheit und des Schutzes der personenbezogenen Daten auf seinem Computer zu genügen,
- die auf dem Computer installierten Programme zu verändern, die ohne vorgeschriebene Tests oder Freigabeverfahren eingesetzt werden und
- Fehlfunktionen verursachen können, ohne dass das Update als Ursache erkannt wird

Dies kann besondere Probleme bei Behörden und Unternehmen in diesem Bereich verursachen, soweit dies speziellen rechtlichen Verpflichtungen beim Umgang mit personenbezogenen Daten Unterliegen.

2. Die Konferenz fordert deshalb die Software-Hersteller dazu auf,:

- a. Verfahren für Online-Programm-Updates nur mit der Benachrichtigung und der Update-Ausübung nach dem Erlangen der Nutzereinstimmung, ohne diese Zustimmung zu übertreten oder verletzen, auf transparente Weise und nur so anzubieten, dass kein unkontrollierter Zugang zum Computer des Nutzers eröffnet wird;
 - b. die Offenbarung von personenbezogenen Daten nur mit der informierten Zustimmung des Nutzers zu verlangen und nur, soweit es zur Durchführung der Aktualisierung erforderlich ist. Die Nutzer dürfen nicht gezwungen werden, ihre Identität zu bestimmen (im Gegensatz zur Authentifizierung) bevor sie das Update herunterladen;
 - c. nur solche Update-Leistungen anzubieten, die die Möglichkeit der vorherigen Prüfung auf einem separaten Server vor der Installation vorsehen.
3. Die Konferenz ruft zur Entwicklung und Umsetzung von solchen Techniken der Aktualisierung von Software auf, die die Privatsphäre und Selbstbestimmung der Computernutzer respektieren.

Erklärungsnoten

Das Ziel des folgenden Dokuments ist die Lieferung der Grundinformationen zum Thema der vorgeschlagenen Änderungen in der während der Konferenz 2003 angenommenen EntschlieÙung zur Automatischen Software-Aktualisierung. Die EntschlieÙung hat aus der Initiative von Alexander Dix entstanden und ist auf der Arbeit der Internationalen Gruppe für Datenschutz in der Telekommunikation basiert worden. Die EntschlieÙung ist auf den www-Seiten der Konferenz 2003 als EntschlieÙung Nr. 4 zu finden:

www.privacyconference2003.org/commissioners.asp

Die EntschlieÙung vom Jahre 2003 hat die Befürchtungen betreffend der Benutzung der nicht-transparenten Techniken bei der Übertragung der Software-Aktualisierungen auf die Computer der Nutzer geäuÙert, was den Softwareproduzenten ermöglichen könnte, die teilweise Kontrolle und den Zugang zu den auf dem Computer des Nutzers gespeicherten Informationen zu gewinnen.

Seit der Veröffentlichung der EntschlieÙung hatte Microsoft den Kontakt mit den mehreren Beauftragten, u. a. mit Alexander Dix, Ann Cavoukian, ihrem Stellvertreter Ken Anderson und dem ehemaligen Australischen Bundesbeauftragten für den Schutz der Privatsphäre Malcolm Crompton. Microsoft hat überzeugende Argumente dafür vorgestellt, dass die bestimmten Teile der während der Konferenz im Jahre 2003 angenommenen EntschlieÙung entweder unmöglich anzuleiten sind, oder die entgegengesetzten zu den beabsichtigten Ergebnisse bringen können. Dies bedeutet, dass die Anleitung der EntschlieÙung die bestimmten Aktualisierungen verspäten könnte, sogar diese, die dringend notwendig sind.

Der Bedarf der schnellen Aktualisierungen ergibt sich aus der Tatsache, dass die mehreren Viren oder Hackerangriffe direkt nach der Veröffentlichung der Software-Aktualisierung stattfinden. Die Hacker und die Virenverfasser finden sehr oft die Software-Schwächen dadurch, dass sie mit der Hilfe von „reverse engineering software updates“ feststellen, was die Software-Aktualisierungen reparieren sollen. In solchen Umständen ist es sehr wichtig, dass die Software-Aktualisierung (manchmal Patch genannt) möglich vielen Personen in der möglich kürzesten Zeit überwiesen wird. Dies unermöglicht den Hackern und Virenverfassern die Ausnutzung der Erwartungszeit, die es zwischen der Veröffentlichung der Software-Aktualisierung und ihrer allgemeinen Annahme gibt, für das Virenschreiben oder für die Angriffe auf schwache Software-Punkte. Wörtlich, jede Verzugsstunde kann zur Vergrößerung der Schaden in der ganzen Welt beitragen.

Die Einstellung der schnellen Software-Aktualisierungsannahme kann zur Verletzung der Privatsphäre dadurch beitragen, dass die Hacker die Zugangsmöglichkeit zu den in den Computern der Nutzer gespeicherten personenbezogenen Daten bekommen.

In Zusammenhang damit hat Microsoft die Menge von den Anmerkungen bezüglich der EntschlieÙung vom Jahre 2003 vorgestellt, die die entgegengesetzten zu den beabsichtigten Ergebnisse betrifft.

Microsoft hat erklärt, was folgt:

„Da die schnelle Verbreitung von Patches sowohl für die Sicherheit des Internets, als auch für seine Benutzer wichtig ist, kann nicht die CD-ROM Distribution einzige Methode sein (d.h. der Teil der Entschlüsselung, der die Online-Aktualisierungen abträgt, ist sehr problematisch). Erstens, die CD-ROM Distribution kann nicht entsprechend schnell durchgesetzt werden, besonders wenn die Würmer im Laufe nur von ein paar Stunden seit der Veröffentlichung des Bulletins gesendet werden. Zweitens, die CD-Platte wird in einem bestimmten Zeitpunkt ausgebrannt und wenn sie von dem Nutzer eingesetzt wird, kann sie nicht mehr aktuell sein (z. B. der Patch konnte schon modifiziert werden oder es konnten die weiteren Patches hergestellt werden). Trotz der Tatsache, dass die Herstellung der CD-Platten brauchbar ist (besonders im Falle der sehr großen Patches oder im Falle der Aktualisierungen des unangepassten Systems durch Sicherung der bestimmten Paketen der Serviceverbesserungen und / oder der Patches), kann nur die Online-Aktualisierung den Nutzern die Möglichkeit der Einsetzung der neusten Patches sichern, bevor das Virus wird das System angreifen oder Hacker wird den unautorisierten Zugang bekommen und PII (Integrierte Information über Software) stehlen.

Es ist für uns nicht klar, warum die Patches nur auf die Bitte oder Initiative des Nutzers geliefert werden sollen, im Gegensatz zum Senden der Benachrichtigungen und zur Sicherung der Auswahl dem Endnutzer. Wir wissen natürlich, dass die einzelnen Fahrer „die Sicherheitsgurte nicht anschnallen“ werden, obwohl dies die Person mit dem Tod oder der schweren Körperverletzung bedroht (ohne zu erwähnen, dass solche Fahrt in bestimmten Jurisdiktionen von der Polizei bestraft werden kann!). Im Licht solcher Wirklichkeit scheint es, dass das sowohl Information, als auch Auswahl bedürftige Verfahren zum Behalten des besseren Gleichgewichtes zwischen Schutz der Privatsphäre durch die Patchsenutzung und Nutzerkontrolle beitragen wird.

Endlich schlagen wir vor, den Text betreffend „den unkontrollierten Zugang“ zu ersetzen, wegen der Tatsache, dass es unklar bleibt, was diese Wendung bedeutet. Das Betriebssystem hat den unkontrollierten Zugang zum System; die Aktualisierung des Betriebssystems (besonders des Kernes des Betriebssystems), das nicht imstande ist, den Zugang zu kontrollieren, scheint sinnlos zu sein. Außerdem, wenn die Patchesbenutzung den Zugang aus der Ebene des Systemverwalters ermöglicht, dann Softwareverkäufer, Verbrecher oder andere Person, die das technische Wissen und Fähigkeiten besitzt, hat „den unkontrollierten Zugang“; darum ist die Patchesbenutzung so wichtig“¹

In der Antwort auf die Anmerkungen von Microsoft hat Alexander Dix zusammen mit den Leuten aus Microsoft an dem Vorschlag der Änderung der Entschlüsselung gearbeitet. Das Ziel war den anfänglichen in der Entschlüsselung vorgesehenen Schutz der Privatsphäre zu behalten, aber auch den oben genannten Schutz anleitmöglich zu machen.

Die veränderte Entschlüsselung ist zusammen mit dem Brief (in dem es erklärt worden ist, warum die Änderung notwendig ist) von dem Australischen Bundesbeauftragten für den Schutz der Privatsphäre ist den Beauftragten am 12. April 2004 zugemailt worden. Leider, nur acht Antworten sind zurückgesendet worden. In solcher Situation ist die Entscheidung getroffen worden, dass es notwendig ist nochmal die Entschlüsselung während der Konferenz zu besprechen und auf solcher Weise ihr den stärkeren Konsensus zu sichern.

Die vorgeschlagene Änderung wird die Entschlüsselung (angenommene während der Konferenz 2003) aus:

1. Die Konferenz fordert deshalb die Software-Hersteller dazu auf:

¹ Die Fragmente aus dem Brief, der von Scott Charney aus Microsoft zu Ann Cavoukian gesendet worden ist. Am 12 April 2004 ist der Brief von dem den Amt des Australischen Bundesbeauftragten für den Schutz der Privatsphäre ausübenden Malcolm Crompton diesen Beauftragten zugemailt worden, die sich mit der Sektion der Entschlüsselung während der Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre im Jahre 2003 beschäftigt haben.

- a. Verfahren für Programm-Updates nur auf die Initiative oder den Wunsch des Nutzers hin, auf transparente Weise und nur so anzubieten, dass kein unkontrollierter Zugang zum Computer des Nutzers eröffnet wird;
- b. die Offenbarung von personenbezogenen Daten nur mit der informierten Einwilligung des Nutzers zu verlangen und nur, soweit es zur Durchführung der Aktualisierung erforderlich ist. Die Nutzer dürfen nicht gezwungen werden, ihre Identität zu bestimmen (in Gegensatz zur Authentisierung) vor dem Anfang des Aktualisierungsherunterladens.
- c. Wahlfreiheit vorzusehen durch das Angebot von Online Updates nur als eine Alternative zu anderen (Offline-) Formen der Software-Distribution wie z.B. auf CD-ROM.

Ins:

- 2. Die Konferenz fordert deshalb die Software-Hersteller dazu auf:
 - a. Verfahren für Programm-Updates nur mit der Benachrichtigung und der Update-Ausübung nach dem Erlangen der Nutzereinstimmung, ohne diese Einwilligung zu übertreten oder verletzen, auf transparente Weise und nur so anzubieten, dass kein unkontrollierter Zugang zum Computer des Nutzers eröffnet wird;
 - b. (nicht verändert)
 - c. nur solche Update-Leistungen anzubieten, die die Möglichkeit der vorherigen Prüfung auf einem separaten Server vor der Einsetzung vorsehen.

verändert.

Als der Veranstalter der Konferenz 2003 schlägt das Büro des Australischen Bundesbeauftragten für den Schutz der Privatsphäre mit der Unterstützung der Beauftragten von Brandenburg, Ontario und Hongkong diese Entschließung vor. Nachdem die Änderungen im April 2004 gesendet worden waren, kriegten sie auch die Unterstützung der Beauftragten von Irland, Spanien, des Deutschen Bundesbeauftragten, des Beauftragten von Niederlanden und des Beauftragten für den Datenschutz der Europäischen Union.

Wenn die Beauftragten die Änderungen der Entschließung akzeptieren werden, werden wir die starke Unterstützung der Industrie mit Microsoft an der Spitze für Implementierung der veränderten Entschließung haben. Dies könnte ein ungewöhnliches Beispiel für „praktischen Schutz der Privatsphäre“ sein, wobei die Beauftragten den bedeutenden Einfluss auf wirkliche weltweite Geschäftspraktiken haben werden.