288/J XXII. GP

Eingelangt am 02.04.2003

Anfrage

der Abgeordneten Mag. Maier
und GenossInnen
an den Bundesminister für Justiz
betreffend Datensicherheitsmaßnahmen im Zusammenhang mit der Verwendung von Microsoft-Produkten - Schutz von personenbezogenen Daten und anderer sensibler oder geheimer Daten, über die Bundesbehörden verfügen.

Die Bundesregierung Schüssel II bekennt sich in ihrem Regierungsprogramm zu einer e-government-Offensive. Dabei sollen die laufenden Projekte abgeschlossen, aber auch neue Initiativen entwickelt werden. Für den Bereich e-government ist es typisch, dass personenbezogene und sensible Daten der Bürgerinnen verarbeitet werden. Aus der Sicht des Datenschutzes kann daher e-government nur dann befürwortet werden, wenn die notwendigen Maßnahmen der Datensicherheit von den Behörden geleistet werden.

In www.golem.de (IT-News für Profis) wurde am 3.2.2003 folgender Artikel veröffentlicht:

„Einblick in Windows-Quellcode für Großbritanniens Regierung
Utl.: Großbritannien unterzeichnet Abkommen über Government Security Programm (GSP)

Nachdem Microsoft Mitte Januar 2003 das so genannte Government Security Programm (GSP) gestartet hatte, unterzeichnete Großbritanniens Regierung nun einen entsprechenden Vertrag. Über das GSP will Microsoft Regierungen und internationalen Institutionen Zugriff auf den Windows-Quelltext bieten.

Microsoft will mit dem Government Security Programm (GSP) vor allem Sicherheitsbedenken aus der Welt räumen. Redmond gesteht, dass sensitive Bürger-Datensammlungen in nationalen Behörden besonders geschützt werden müssen. Gemäß des GSP erhält Großbritannien nun vertrauliche technische Unterlagen über das Windows-

Betriebssystem sowie einen besseren Kontakt zu den Sicherheits-Profis bei Microsoft. Außerdem steht es der Regierung frei, die Entwicklungsabteilungen in Redmond zu besuchen sowie zahlreiche Aspekte des Windows Quellcodes mit Microsoft zu besprechen.

Bereits mit der Ankündigung des GSP hatte nach Microsoft-Angaben die Russische Behörde für Regierungskommunikation und - information (FAGCI) und die NATO ein GSP-Abkommen unterzeichnet. Nun folgt Großbritanniens Regierung als dritter Vertragspartner."

In der Homepage von Microsoft ist folgende ergänzende Informationen verfügbar:

„Programm ermöglicht stabile Sicherheitsüberwachung der Windows-Plattform Microsoft kündigt Sicherheits-initiative für Behörden an

Behörden sind Sicherheitsbedrohungen in noch höherem Maße ausgesetzt als andere Technologie-Kunden. Ob Landesverteidigung oder Datenschutz, die Sicherheit der IT-Infrastruktur hat bei Behörden oberste Priorität. Microsoft hat daher das Government Security Program (GSP) ins Leben gerufen, eine weltweite Initiative, mit der nationale Behörden einen kontrollierten Zugriff auf den Quellcode des Betriebssystems Microsoft Windows erhalten. Darüber hinaus werden technische Informationen zur Verfügung gestellt, mit denen die erweiterten Sicherheitsfunktionen der Windows-Plattform in vollem Umfang genutzt werden können.

Das GSP spielt eine wichtige Rolle im Rahmen des Engagements von Microsoft, den besonderen Sicherheitsanforderungen von Behörden und internationalen Organisationen Rechnung zu tragen. Russland und die NATO haben bereits entsprechende Vereinbarungen mit Microsoft unterzeichnet. Derzeit befindet sich Microsoft mit mehr als 20 interessierten Ländern in Verhandlungen. Die Teilnahme am GSP wird nach Ermessen des entsprechenden Landes offengelegt. Microsoft sichert hier absolute Vertraulichkeit zu.
Boris Girichev, General Director von Atlas, der von der Federal Agency for Governmental Communication and Information (FAGVCI) mit der Unterzeichnung der GSP-Vereinbarung beauftragt wurde, erläutert: „Diese Vereinbarung ist ein wichtiger Schritt, den Sicherheitsanforderungen unserer IT nachzukommen. Die Behörden der Russischen Föderation sind damit optimal gerüstet, sichere Computerinfrastrukturen zu implementieren und zu betreiben."
Einblick in den Quellcode von Microsoft Windows
Während einige Microsoft Quellcode-Lizenzierungsprogramme für jedermann offen stehen, wurde das Government Security Program auf die speziellen Sicherheitsanforderungen von Behörden zugeschnitten. Im Rahmen der kostenfreien Initiative erhalten die Teilnehmer unter Berücksichtigung bestimmter Lizenzbeschränkungen Einblick in den Quellcode von Windows. Neben dem Quellcode werden technische Informationen über die Windows Plattform offen gelegt. Damit sind Behörden in der Lage, ihre IT-Infrastrukturen mit umfangreichen Sicherheitstechnologien auszustatten.

Im Rahmen der Initiative erfolgt eine enge Zusammenarbeit zwischen den Sicherheitsexperten von Microsoft und den Teilnehmern des Programms. So haben die Teilnehmer Gelegenheit, die Entwicklungslabors von Microsoft in Redmond zu besuchen und dort Einblicke in die Entwicklung des Windows Quellcodes sowie in Test- und Entwicklungsprozesse zu bekommen. Diskussionen mit den Sicherheitsexperten über bestehende und zukünftige Projekte sind ebenfalls möglich.
Das Government Security Program trägt dem Bestreben von Microsoft Rechnung, die besonderen Anforderungen von Behörden weltweit zu berücksichtigen. Um ausgewählten Partnern und Kunden den Windows Quellcode transparenter zu machen, hat Microsoft im Jahr 2001 die Shared Source Initiative ins Leben gerufen. Die im Jahr 2002 gestartete Initiative Trustworthy Computing stellt den Faktor Sicherheit in den Mittelpunkt sämtlicher Windows-Entwicklungen.

Unterstützung des Konzepts Common Criteria

Das Government Security Programm unterstützt auch die Common-Criteria- Zertifizierung (CC), ein weltweit akzeptierter Standard für die Bewertung der Sicherheitseigenschaften von IT-Produkten. Das Betriebssystem Windows 2000 hat die CC-Zertifizierung im Oktober letzten Jahres erhalten. Windows 2000 hat seine Fähigkeiten auch in den anspruchsvollsten Real-World-Szenarien unter Beweis gestellt. Die Bewertung erfolgte nach den offiziellen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationssystemen.
Während das Konzept Common Criteria Anwendern einen objektiven Maßstab für die Vertrauenswürdigkeit und Sicherheit von IT-Produkten und -Systemen liefert, geht das GSP noch einen Schritt weiter: Es stellt nationalen Behörden die Informationen zur Verfügung, die für eine stabile Sicherheitsanalyse und -Überwachung der Microsoft Windows-Produkte erforderlich sind.
Craig Mundie, Chief Technology Officer und Senior Vice President for Advanced Strategies and Policy bei Microsoft, erläutert: ‚Wir betrachten Behörden, die unsere Software einsetzen, als vertrauenswürdige Partner. Das Government Security Program bietet Behörden die Möglichkeit, die Sicherheit und Integrität ihrer Microsoft Produkte zu überprüfen. In Gesprächen mit Kunden hat sich herausgestellt, dass dies eine sehr wichtige Anforderung ist, auf die wir entsprechend reagiert haben. Neben dem Zugang zum Quellcode stellen wir technische Dokumentationen zur Verfügung, Methoden für die Fehlersuche sowie kryptographische Tools. Außerdem unterstützen unsere Support-Techniker die Behörden dabei, den Quellcode sinnvoll zu nutzen.'
Weitere Informationen:
http://www.microsoft.com/presspass
http://www.microsoft.com/sharedsource
http://www.microsoft.com/security"

Es handelt sich bei diesen Government Security Program um eine völlig neue Entwicklung, die zwischen verschiedenen Staaten und Microsoft im Jänner 2003 gestartet wurde, um die Datensicherheit aller eingesetzten Microsoft-Produkte von Behörden zu erhöhen. Auch die österreichischen Behörden verfugen über eine Reihe von sensiblen personenbezogenen Daten oder anderen Daten, die aus verschiedenen Gründen im Interesse der Republik geheim sind.

Die anfragestellenden Abgeordneten würden es daher im Sinne des Datenschutzes begrüßen, wenn auch Österreich ein solches Programm gemeinsam mit Microsoft beginnen würden, um die dort gespeicherten Daten in einem besseren Ausmaß als bisher schützen zu können. Wie schon in der Einleitung dargestellt, ist für ein funktionierende e-government aus der Sicht des Datenschutzes unabdingbar notwendig, dass alle möglichen Maßnahmen von Seiten der Behörden gesetzt werden, um höchste Datensicherheit zu garantieren.

Die unterzeichneten Abgeordneten richten daher an das im Kopf der Anfrage genannte Mitglied der Bundesregierung nachstehende

Anfrage:

1. Welche personenbezogenen Daten werden in Ihrem Ressort ermittelt und EDV-mäßig verarbeitet und gespeichert? Durch welche konkrete Rechtsgrundlage ist dies jeweils gedeckt?
2. Welche Daten, die von Ihrem Ressort ermittelt oder verarbeitet werden, sind im Sinne des Datenschutzgesetzes 2000 sensible Daten? Welche Organisationseinheiten von Bundesministerien, Gebietskörperschaften oder anderer Einrichtungen haben darauf einen Zugriff?
3. Ist Ihnen bekannt, ob Österreich ein Government Security Program mit Microsoft begonnen hat bzw. beabsichtigt, ein solches zu beginnen?
4. Welche Rolle spielt dabei Ihr Ressort?
5. Haben Sie bereits einen kontrollierten Zugriff auf den Quellcode des Betriebssystems Microsoft Windows erhalten?
6. Wenn ja, welche Maßnahmen haben Sie aufgrund dieser Kenntnisse gesetzt?
7. Welche Datensicherheitsmaßnahmen sehen Sie in Ihrem Ressort vor?

8. Welche Daten werden verschlüsselt?

9. Wird der E-mail-Verkehr verschlüsselt?

10. Stehen Sie in Kontakt mit ausländischen Behörden (EU und Drittstaaten), die Daten Ihres Ressorts übermittelt bekommen wollen?

11. Wenn ja, welche Daten wurden 2000, 2001, 2002 und 20003 von wem angefragt?

12. Wenn ja, welche Daten wurden 2000, 2001, 2002 und 20003 auf welcher Rechtsgrundlage übermittelt?

13. Hatten Sie oder Ihr Ressort insbesondere Kontakt mit dem amerikanischen Information Awareness Office (IAO)?

14. Wenn ja, welche Daten wurden vom IAO konkret verlangt?

15. Wenn ja, haben Sie Daten dem IAO übermittelt (aufgeschlüsselt nach allen Datenkriterien)? Wann haben Sie diese jeweils übermittelt?

16. Wenn ja, welche Rechtsgrundlage wurde für die Übermittlung herangezogen?

17. Welche Microsoft-Produkte werden in Ihrem Ressort eingesetzt?

18. Wenn Microsoft-Produkte eingesetzt werden, wissen Sie, welche Daten tatsächlich an Microsoft übertragen werden und ob sich aus diesen Daten Nutzungsprofile der Anwender erstellen lassen oder personenbezogene Daten, die einem besonderen Schutz unterliegen (sensibel) mitübertragen werden?

19. Haben Sie, wie z.B. vom Datenschutzbeauftragten Mecklenburg-Vorpommerns empfohlen, vor der Einsatzplanung von Microsoft-Produkten wie Windows-XP ein Sicherheitskonzept erstellt? Wenn nein, warum nicht?

20. Welche zusätzlichen Sicherheitsmaßnahmen werden Sie im Rahmen der Fortsetzung des e-government-Projektes setzen, um eine höchste Datensicherheit im Sinne der Bürgerinnen zu gewährleisten?