Microsoft

Microsoft Blog Statements

Über den Schutz von Kundendaten vor dem Ausspähen durch Regierungen

Veröffentlicht von Brad Smith,
General Counsel & Executive Vice President, Legal & Corporate Affairs, Microsoft
4. Dez. 2013 21:00 Uhr

Der folgende Artikel ist eine Übersetzung des von Microsoft im Blog Technet am 04.12.2013 veröffentlichten Artikels
Protecting customer data from government snooping

Über den Schutz von Kunden-daten vor dem Ausspähen durch Regierungen

Veröffentlicht von Brad Smith,
General Counsel & Executive Vice President, Legal & Corporate Affairs, Microsoft
04.12.2013

Viele unserer Kunden haben ernsthafte Bedenken im Hinblick auf die staatliche Überwachung des Internets. Wir teilen ihre Bedenken. Deshalb unternehmen wir Schritte, um sicherzustellen, dass Regierungen den vorgeschriebenen Rechtsweg einhalten statt die technologische „Brute-Force-Methode" anzuwenden, um Zugang zu Kundendaten zu erhalten.

Wie viele andere sind auch wir alarmiert von den neuesten Behauptungen in der Presse über weiterreichende und abgestimmte Anstrengungen einiger Regierungen zur Umgehung von Sicherheitsmaßnahmen im Internet – und unserer Ansicht nach auch zur Umgehung von rechtlichen vorgesehenen Verfahren und Rechtsschutz – um heimlich private Kundendaten zu sammeln. In den neuesten Pressemeldungen wurde insbesondere Behauptungen wieder gegeben, dass der Staat – ohne Durchsuchungsbefehle oder rechtmäßige Herausgabeanordnungen – Kundendaten abfängt und sammelt während sich diese zwischen den Kunden und Servern oder zwischen Datenzentren von Unternehmen unserer Branche hin und her bewegen.

Sollte dies wahr sein, drohen diese Bemühungen das Vertrauen in die Sicherheit und die Privatsphäre von Internet-Kommunikation ernsthaft zu untergraben. Tatsächlich stellt das staatliche Ausspionieren potenziell eine „fortgeschrittene, andauernde Bedrohung" dar, ebenso wie hochentwickelte Schadsoftware und Cyberangriffe.

Angesichts dieser Behauptungen haben wir uns dazu entschieden, sofort und koordiniert Maßnahmen in drei Bereichen zu ergreifen:

Wir bauen die Verschlüsselung in unseren Diensten aus.

Wir verstärken den Rechtsschutz für die Daten unserer Kunden.

Wir optimieren die Transparenz unseres Quellcodes der Software, sodass es Kunden leichter fällt, sich davon zu überzeugen, dass es bei unseren Produkten keine Hintertüren gibt.

Wir geben nachfolgend einen Einblick in unsere Maßnahmen :

Ausbau der Verschlüsselung

Seit vielen Jahren verwenden wir bei unseren Produkten und Diensten Verschlüsselung, um unsere Kunden vor Kriminellen und Hackern im Internet zu schützen. Obwohl wir keinen unmittelbaren Beweis dafür haben, dass Kundendaten von einem unzulässigen staatlichen Zugriff betroffen waren, wollen wir keine Risiken eingehen und befassen uns direkt mit diesem Problem. Daher werden wir umfangreiche technische Maßnahmen ergreifen, um die Verschlüsselung von Kundendaten in unseren Netzwerken und Diensten zu verstärken.

Diese Maßnahmen umfassen unsere wichtigsten Kommunikations- sowie Produktivitäts- und Entwicklerdienste, wie beispielsweise Outlook.com, Office 365, SkyDrive und Windows Azure, und werden die von den Kunden erstellten Inhalte während ihres gesamten Lebenszyklus schützen. Im Einzelnen:

Zwischen unseren Kunden und Microsoft hin und her bewegte Kundeninhalte werden standardmäßig verschlüsselt.

All unsere wichtigen Plattformen sowie Produktivitäts- und Kommunikationsdienste werden zwischen unseren Datenzentren hin- und her bewegte Kundeninhalte verschlüsseln.

Wir werden die „best-in-class" Verschlüsselungstechnik der Branche verwenden, um diese Kanäle zu schützen, einschließlich der sog. Perfect Forward Secrecy Methode und 2048-bit Schlüssellänge.

All dies wird bis Ende 2014 umgesetzt und Einiges ist sofort wirksam.

Wir werden auch von uns gespeicherten Kundeninhalt verschlüsseln. In einigen Fällen, wie beispielsweise Dienste Dritter, die für Windows Azure programmiert wurden, überlassen wir zwar die Entscheidung den Entwicklern, aber wir werden die Tools anbieten, die es ihnen ermöglichen, die Daten einfach zu schützen.

Wir arbeiten mit anderen Unternehmen der Branche zusammen, um sicherzustellen, dass Daten geschützt sind, die zwischen den Diensten – beispielsweise zwischen E-Mail-Providern - hin und her bewegt werden.

Auch wenn dies angesichts der großen Anzahl der von uns angebotenen Dienste und den Hunderten von Millionen von uns bedienten Kunden eine enorme technische Anstrengung bedeutet, sind wir entschlossen, dies alles schnell umsetzen. In der Tat profitieren viele unserer Dienste bereits von der starken Verschlüsselung im gesamten oder in Teilen des Lebenszyklus. Zum Beispiel ist der Kundeninhalt bei Office 365 und Outlook.com bereits verschlüsselt, wenn er sich zwischen den Kunden und Microsoft bewegt, und ein Großteil der Office 365 Anwendungsmöglichkeiten sowie der Speicher von Windows Azure sind bei der Weiterleitung zwischen unseren Datenzentren inzwischen verschlüsselt. In anderen Bereichen beschleunigen wir die Pläne zum Einsatz von Verschlüsselung.

Stärkung des Rechtsschutzes

Wir werden auch neue Schritte zur Stärkung des Rechtsschutzes für die Daten unserer Kunden unternehmen. Wir haben uns zum Beispiel dafür entschieden, Geschäfts- und Regierungskunden zu informieren, wenn wir rechtmäßige Verfügungen in Bezug auf ihre Daten erhalten. Wenn ein Offenlegungsverbot uns daran hindert, dies zu tun, werden wir dieses vor Gericht anfechten. Wir haben damit in der Vergangenheit Erfolg gehabt und werden dies in Zukunft genauso handhaben, um uns die Möglichkeit zu erhalten, Kunden zu warnen, wenn Regierungen versuchen, an ihre Daten heranzukommen. Und wir werden gegenüberrechtmäßigen Anforderungen mögliche Zuständigkeitsrügen erheben, wenn Regierungen Inhalte von Kunden anfordern, die in einem anderen Land gespeichert sind.

Wir sind der Auffassung, dass Regierungsbehörden – außer unter sehr eng begrenzten Umständen - selbst direkt auf Geschäfts- und Regierungskunden zugehen können, wenn es um Informationen oder Daten über einen ihrer Mitarbeiter geht – genauso wie sie dies getan haben, bevor diese Kunden anfingen, die Cloud zu nutzen – ohne dass sie dabei ihre Ermittlungen oder die nationale Sicherheit untergraben. Und wenn einmal diese sehr eng begrenzten Umstände eintreten, sollen Gerichte die Möglichkeit haben, die Frage zu überprüfen und eine Entscheidung zu erlassen.

Erhöhung der Transparenz

Genauso wie wir Regierungen aufgefordert haben, im Hinblick auf diese Fragestellungen transparenter zu werden, sind wir der Auffassung, dass es für uns selbst angemessen ist, transparenter zu sein. Wir unternehmen daher zusätzliche Schritte, um die Transparenz zu erhöhen, und zwar aufbauend auf unser langjähriges Programm, das es Regierungskunden in angemessener Weise ermöglicht, unseren Quellcode einzusehen, sich von seiner Integrität zu überzeugen und sich zu vergewissern, dass es keine Hintertüren gibt. Wir werden ein Netzwerk von Transparenz-Zentren eröffnen, das es diesen Kunden in noch größerem Umfang ermöglichen wird, sich selbst von der Integrität der Produkte von Microsoft zu überzeugen. Wir werden diese Zentren in Europa, Nord- und Südamerika und Asien eröffnen und wir werden die Auswahl der darin enthaltenen Produkte erhöhen.

Schlussendlich sind wir uns darüber im klaren, dass Technologie, Sicherheit und das Gesetz in Einklang zu bringen sind. Wir wollen alle in einer sicheren und geschützten Welt leben, aber wir wollen auch in einem Land leben, das durch die Verfassung geschützt ist. Wir wollen sicherstellen, dass die wichtigen Fragen über den staatlichen Zugriff von Gerichten entschieden und nicht durch technologische Macht diktiert werden. Und unser Fokus liegt darauf, weltweit neue Schutzmaßnahmen zu ergreifen, die dem globalen Charakter dieser Fragestellungen und Herausforderungen gerecht werden. Wir sind der Auffassung, dass diese neuen Schritte die richtige Gewichtung haben, um für uns alle sowohl die Sicherheit zu erhöhen, die wir benötigen, als auch die Privatsphäre, die wir verdienen.

Originaltext

Protecting customer data fromgovernment snooping

Posted by Brad Smith,
General Counsel & Executive Vice President, Legal & Corporate Affairs, Microsoft,
4 Dec 2013 9:00 PM

Many of our customers have serious concerns about government surveillance of the Internet.

We share their concerns. That's why we are taking steps to ensure governments use legal process rather than technological brute force to access customer data.

Many of our customers have serious concerns about government surveillance of the Internet.

We share their concerns. That's why we are taking steps to ensure governments use legal process rather than technological brute force to access customer data.

Like many others, we are especially alarmed by recent allegations in the press of a broader and concerted effort by some governments to circumvent online security measures – and in our view, legal processes and protections – in order to surreptitiously collect private customer data. In particular, recent press stories have reported allegations of governmental interception and collection – without search warrants or legal subpoenas – of customer data as it travels between customers and servers or between company data centers in our industry.
If true, these efforts threaten to seriously undermine confidence in the security and privacy of online communications. Indeed, government snooping potentially now constitutes an "advanced persistent threat," alongside sophisticated malware and cyber attacks.

In light of these allegations, we've decided to take immediate and coordinated action in three areas:

We are expanding encryption across our services.

We are reinforcing legal protections for our customers' data.

We are enhancing the transparency of our software code, making it easier for customers to reassure themselves that our products do not contain back doors.

Here's a closer look at what we're doing:

Expanding Encryption

For many years, we've used encryption in our products and services to protect our customers from online criminals and hackers. While we have no direct evidence that customer data has been breached by unauthorized government access, we don't want to take any chances and are addressing this issue head on.

Therefore, we will pursue a comprehensive engineering effort to strengthen the encryption of customer data across our networks and services.This effort will include our major communications, productivity and developer services such as Outlook.

com, Office 365, SkyDrive and Windows Azure, and will provide protection across the full lifecycle of customer-created content. More specifically:

Customer content moving between our customers and Microsoft will be encrypted by default.

All of our key platform, productivity and communications services will encrypt customer content as it moves between our data centers.

We will use best-in-class industry cryptography to protect these channels, including Perfect Forward Secrecy and 2048-bit key lengths.

All of this will be in place by the end of 2014, and much of it is effective immediately.

We also will encrypt customer content that we store. In some cases, such as third-party services developed to run on Windows Azure, we'll leave the choice to developers, but will offer the tools to allow them to easily protect data.

We're working with other companies across the industry to ensure that data traveling between services – from one email provider to another, for instance – is protected.

Although this is a significant engineering effort given the large number of services we offer and the hundreds of millions of customers we serve, we're committed to moving quickly. In fact, many of our services already benefit from strong encryption in all or part of the lifecycle. For example, Office 365 and Outlook.com customer content is already encrypted when traveling between customers and Microsoft, and most Office 365 workloads as well as Windows Azure storage are now encrypted in transit between our data centers. In other areas we're accelerating plans to provide encryption.

Reinforcing Legal Protections

We also will take new steps to reinforce legal protections for our customers' data. For example, we are committed to notifying business and government customers if we receive legal orders related to their data. Where a gag order attempts to prohibit us from doing this, we will challenge it in court. We've done this successfully in the past, and we will continue to do so in the future to preserve our ability to alert customers when governments seek to obtain their data. And we'll assert available jurisdictional objections to legal demands when governments seek this type of customer content that is stored in another country.

Except in the most limited circumstances, we believe that government agencies can go directly to business customers or government customers for information or data about one of their employees – just as they did before these customers moved to the cloud – without undermining their investigation or national security. And when those limited circumstances arise, courts should have the opportunity to review the question and issue a decision.

Increasing Transparency

Just as we've called for governments to become more transparent about these issues, we believe it's appropriate for us to be more transparent ourselves. We're therefore taking additional steps to increase transparency by building on our long-standing program that provides government customers with an appropriate ability to review our source code, reassure themselves of its integrity, and confirm there are no back doors. We will open a network of transparency centers that will provide these customers with even greater ability to assure themselves of the integrity of Microsoft's products. We'll open these centers in Europe, the Americas and Asia, and we'll further expand the range of products included in these programs.

Ultimately, we're sensitive to the balances that must be struck when it comes to technology, security and the law. We all want to live in a world that is safe and secure, but we also want to live in a country that is protected by the Constitution. We want to ensure that important questions about government access are decided by courts rather than dictated by technological might. And we're focused on applying new safeguards worldwide, recognizing the global nature of these issues and challenges. We believe these new steps strike the right balance, advancing for all of us both the security we need and the privacy we deserve.

Originalpost:
http://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/