Microsoft Security Development Lifecycle (SDL)

November 2010

Hintergrund

Die heutigen Angriffe auf die Cybersicherheit sind komplex, äußerst durchdacht und verändern sich ständig. Das heißt, dass kontinuierliche und vielfältige Anstrengungen notwendig sind, eine sichere Nutzung von Computern und des Internets zu ermöglichen.

Der Microsoft Security Development Lifecycle (SDL) ist Microsofts Qualitätssicherungsprozess für die Softwareentwicklung, der umfassende Antworten auf Sicherheitsbedrohungen und die zunehmende Professionalisierung von Cyberkriminalität liefert. Der SDL kombiniert einen ganzheitlichen und gleichzeitig praxisorientierten Ansatz, um Sicherheit und Datenschutz in allen Phasen des Entwicklungsprozesses zu gewährleisten. Ziel dabei ist es, die Sicherheit der Software zu optimieren und die Kunden weltweit optimal zu schützen.

Seit der Einführung des SDL im Jahr 2004 konnte Microsoft die Schwachstellen in Produkten wie Windows Vista®, Microsoft Office, und Microsoft SQL Server™ erheblich reduzieren. Darüber hinaus haben wir festgestellt, dass diese chronologischen Prozesse, die im SDL beschrieben sind, mehr Sicherheit für Unternehmen schaffen und gleichzeitig den Kostenaufwand reduzieren. Die Ressourcen für den SDL umfassen Tools, Informations- und Trainingsmaterial und Prozessbeschreibungen. Microsoft stellt Softwareentwicklern, Partnern und anderen Unternehmen der IT-Industrie diese Werkzeuge kostenfrei zur Verfügung.

Microsofts Lösungsansatz

Microsoft entwickelte den SDL-Prozess im Jahr 2004 als Teil einer integrierten und durchgängigen Sicherheitsarchitektur. Ziel ist es, die Zahl der Schwachstellen in der Software zu reduzieren und Kunden eine hochqualitative, sorgfältig entwickelte und umfassend getestete Software anzubieten, die optimalen Schutz vor Angriffen bietet.

Der SDL umfasst eine Folge von sicherheitsrelevanten Aktivitäten und Aktionen. Hierzu zählen unter anderem technische Trainings und fortlaufende Weiterbildung, Softwaredesign und -entwicklung, Code-Reviews sowie Sicherheits- und Datenschutztests.

Obwohl es nicht machbar ist, alle Schwachstellen im Softwareentwicklungsprozess vollständig auszumerzen, ist es dennoch möglich, für ein Maximum an Schutz zu sorgen, wenn Schwachstellen zutage treten. Softwareentwicklung ist ein Prozess, der sich kontinuierlich verändert. Bei jeder entdeckten Schwachstelle erlaubt es der SDL nachzuvollziehen, welche Stelle im Entwicklungsprozess die Ursache für diese Schwachstelle ist. Dieses Wissen fließt dann wiederum in die nächste Version des SDL ein.

Weiterführende Informationen:

www.microsoft.com/sdl
Microsoft Security Development Lifecycle

www.microsoft.com/security
Allgemeine Informationen zu Schutz und Online-Sicherheit

Microsoft aktualisiert den SDL regelmäßig, um das Wissen und praxisbewährte Methoden aus allen Phasen des Softwareentwicklungsprozesses einfließen zu lassen. Seitdem der SDL für die Softwareentwicklung genutzt wird, konnten wir messbare Verbesserungen der Sicherheit in unserer Software feststellen:

- Im ersten Jahr nach dem Verkaufsstart von Windows Vista konnten wir 66 Schwachstellen feststellen. Bei Windows XP waren es im Vergleich hierzu 119 Schwachstellen – das sind 45 Prozent weniger (Quelle: Windows Vista Once Year Vulnerability Report).
- Ein Jahr nachdem der Microsoft Internet Explorer® 7 auf den Markt kam, zeigte der Browser lediglich 17 Schwachstellen. Im Microsoft Internet Explorer 6 fanden sich noch 26 Schwachstellen. Insgesamt konnte Microsoft die Zahl der Schwachstellen in den eigenen Lösungen um 35 Prozent senken. Die Zahl der Schwachstellen mit mittlerem und hohem Sicherheitsrisiko ließ sich um 65 Prozent reduzieren (Source: Internet Explorer Vulnerability Analysis Report). Da Kriminelle zielgerichtet die Reichweite ihrer Angriffe ausdehnen und die Anzahl weiter erhöhen werden, werden wir auch weiterhin die Anzahl und die Schwere der Schwachstellen in unseren Produkten reduzieren und somit sicherstellen, dass wir unseren Kunden eine vertrauenswürdige Plattform zur Verfügung stellen. Wir engagieren uns für sichere, verlässliche Software. Mit dem SDL haben wir einen branchenführenden Qualitätssicherheitsprozess entwickelt, um dies zu gewährleisten.

Die wichtigsten Punkte im Überblick

Der Microsoft SDL umfasst technologische wie auch organisatorische Prozesse und führt durch jeden Schritt im Software-Entwicklungszyklus.

Der SDL-Prozess

- schafft in jeder Phase der Softwareentwicklung Sicherheit und bietet einen „Defense-in-Depth"-Leitfaden für maximalen Schutz;
- ist ebenso ein Bottom-up-Prozess wie auch ein Top-down-Prozess, wobei die Security-Teams für Office, Windows®, SQL Server sowie andere Produktlinien an Innovationen arbeiten, die in die SDL-Richtlinien einfließen und für die Öffentlichkeit zugänglich sind;
- ist ein System bestehend aus Anforderungen und Technologien, das sich kontinuierlich weiterentwickelt, verbessert und regelmäßig alle sechs Monate aktualisiert wird, um von technischen Entwicklungen zu profitieren;
- ist nicht Microsoft-spezifisch oder nur für Windows-Plattformen gültig. Der SDL-Prozess kann für verschiedene Betriebssysteme, Plattformen, Methoden der Softwareentwicklung und Projekte jeder Größenordnung eingesetzt werden.

Microsoft möchte Kunden schützen und eine sichere Plattform für Computer und das Internet schaffen. Ein Weg ist es, Erfahrungen, Leitlinien, Technologien und Prozesse auszutauschen. Deshalb stellen wir die SDL-Ressourcen – Tools, Trainings und Methoden – Partnern und Organisationen weltweit zur Verfügung.