



Microsoft Security Development Lifecycle (SDL)

Der Microsoft Security Development Lifecycle (SDL), der von Microsoft im Jahr 2004 entworfen und intern implementiert wurde, ist ein bahnbrechender Prozess für die Entwicklung von sicherer Software. Durch SDL können sicherheitsrelevante Mängel weitgehend ausgeschlossen und Folgeschäden durch Design- und Programmierfehler reduziert werden.

Angesichts der Tatsache, dass sich Angriffe in zunehmendem Maße gegen Applikationen richten, hat sich Microsoft dazu entschlossen, SDL auch externen Entwicklern zur Produktion von sicherer Software zur Verfügung zu stellen.



Lesen Sie hierzu bitte auch: <http://msdn.microsoft.com/en-us/security/cc448177.aspx>

Hintergrund

Die stetig steigende Zahl von Angriffen auf die Applikationsebene stellt eine dramatische Bedrohung für die sicherheitskritischen Daten Ihrer Kunden dar.

Microsoft sah sich über viele Jahre mit diesen Herausforderungen konfrontiert und führte als Antwort darauf mit dem SDL eine äußerst wirksame Methodik ein, die sich in einer deutlich geringeren Anzahl von Schwachstellen bei Microsoft Flaggschiff-Produkten, wie z.B. VISTA, niederschlug und somit einen optimierten Schutz von Kunden gegen bösartige und kostenintensive Attacken bot.

SDL hat sich bei Microsoft als effektives Sicherheitsinstrument bewährt – Jetzt können Sie mit n.runs als Partner denselben Prozess erfolgreich auch in Ihrer Organisation einsetzen

Über die letzten Jahre hinweg konnte sich n.runs einen erstklassigen Namen für die erfolgreiche Implementierung von Security Development Lifecycle Services bei Kunden aus den unterschiedlichsten Bereichen machen. Die Kernelemente der n.runs Trainings und Beratung in diesem Umfeld kommen dem Microsoft SDL sehr nahe, so dass wir neben der entsprechenden Expertise auch über die notwendigen Ressourcen verfügen, um Sie ab sofort professionell bei Implementierung und Betrieb zu unterstützen. Dies war einer der Gründe, warum Microsoft n.runs als einziges zentraleuropäisches Mitglied in das Microsoft SDL Pro Network berufen hat.

Unsere SDL Services

Unsere SDL Services stehen Unternehmen jeder Größenordnung zur Verfügung. Eng angelehnt an den SDL umfassen sie den kompletten Lifecycle und machen Security und Datensicherheit zu einem integralen Bestandteil des Software-Entwicklungsprozesses.

n.runs stellt Ihnen folgende dezidierte SDL Services zur Verfügung:

- **Training, Richtlinien und Organisation**, beinhaltet u.a. Security Training, Richtlinien für sichere Programmierung oder generelle Beratung zum holistischen SDL Prozess
- **Anforderung, Spezifikation und Design**, beinhaltet u.a. Risiko Analyse (Threat Modeling) oder funktionelle Voraussetzungen
- **Implementierung**, beinhaltet u.a. Quellcode Analyse (statische und manuelle), Anwendung von sicheren APIs oder Umsetzung der Richtlinien
- **Verifizierung**, beinhaltet u.a. Kontrollmechanismen für die Umsetzung der Richtlinien, automatisierte Schwachstellenfindung (Scanning) oder Fuzzing
- **Veröffentlichung und Reaktion**, beinhaltet u.a. Finale Durchsicht (Final Security Review), Penetration Testing oder Reaktion und Maßnahmenkatalog bei einer externen Schwachstellenfindung

Hier nur einige Ihrer Vorteile durch SDL:

- Reduzierung des Kundenrisikos und somit starke Vertrauensbildung durch Lieferung von Software, die unternehmenskritische Informationen durch einen hohen Sicherheitsstandard schützt
- Reduzierung der Entwicklungskosten durch frühes Auffinden und Beseitigen von Schwachstellen bereits in der Designphase, was laut NIST (National Institute of Standards and Technology) eine Ersparnis von mehr als 30 % gegenüber einer Beseitigung nach dem Release bedeutet.
- Reduzierung der Cost of Ownership durch die Ausgabe von weniger Security Patches und somit eine Kostenreduzierung durch verringertes Patch Management für Ihre Applikationen.

Für weitere Informationen und Beratung steht Ihnen unser SDL-Team unter Email sdl@nruns.com oder Tel 0049 (0)6171/699-0 gerne zur Verfügung.