Linksrutsch in der Sicherheits-kultur

FACHARTIKEL

_DANIEL ESTERMANN
Product Marketing Manager Airlock
Ergon Informatik AG
_ROMAN HUGELSHOFER
Managing Director Application Security
Ergon Informatik AG

Erschienen im SMART insights 2021 Magazin

ergon

smart people – smart software®

Damit Ideen schnell ausprobiert und Feedback früh eingeholt werden kann, arbeiten Entwicklung, Security und Betrieb gemeinsam im gleichen Team. Dabei werden Security-Tools automatisch in jede Phase des Software-Entwicklungs-Lebenszyklus eingebunden. Das Resultat: sichere Software mit der Geschwindigkeit von Agile und DevOps. Security wird damit Kostensparer und Beschleuniger zugleich.

Um schneller auf neue Herausforderungen reagieren zu können, werden Unternehmen zunehmend agiler und kund:innenorientierter. Kund:innen fordern heute die besten Services und Features – jederzeit verfügbar, einfach bedienbar und sicher. Die Bedürfnisse werden künftig nicht weniger, das Tempo nicht langsamer und die Komplexität nicht geringer. Um Spitzenleistungen zu erzielen, müssen Unternehmen Silos aufbrechen und Legacy-Prozesse neu denken.

Agile und DevOps sind bereits wichtige Weiterentwicklungen des Software-Entwicklungsprozesses. Sie machen Unternehmen schneller und handlungsfähiger. Mit DevSecOps – kurz für Entwicklung, Sicherheit und Betrieb – folgt der nächste Evolutionsschritt. Denn vereint und aligniert, erreichen Agile und DevSecOps ihr gemeinsames Ziel: die bestmögliche Kund:innenerfahrung und kurze Bereitstellungszyklen.

Aller guten Dinge sind drei

DevSecOps stellt eine natürliche und notwendige Entwicklung dar, wie Unternehmen bei der Software-Entwicklung das Thema Sicherheit angehen können. Es automatisiert die Integration von Cybersecurity in jeder Phase der Software-Entwicklung. Vom ersten Entwurf über Integration, Tests und Bereitstellung bis hin zur Auslieferung der Software. DevSecOps ist eine Erweiterung von DevOps. Beide Methoden weisen ähnliche Merkmale auf, darunter die Automatisierung und die Verwendung von kontinuierlichen Prozessen zur Etablierung kollaborativer Entwicklungszyklen. Während DevOps die Liefergeschwindigkeit priorisiert, setzt DevSecOps auf die Security. Das Thema Sicherheit rutscht damit im Entwicklungszyklus zeitlich nach links, ist also von Beginn an eingebettet.

In der Vergangenheit wurde Security am Ende des Entwicklungszyklus von einem separaten Team fast wie ein Nachgedanke an die Software «angeheftet» und von einem weiteren Team getestet.

Früher, als Software-Updates nur ein- oder zweimal im Jahr veröffentlicht wurden, war dies noch überschaubar. Doch mit der Etablierung von Agile- und DevOps-Praktiken, die auf schnelle Releases innert Tagen oder Wochen abzielen, reicht dieser nachgelagerte Security-Ansatz nicht mehr aus.

Das Ziel ist es, Applikationen von Beginn an kontinuierlich zu schützen und dazu die Security nach vorne zu verlagern. Schwachstellen und Sicherheitsrisiken sollen also nicht erst am Ende, sondern bereits zu Beginn und während der Software-Entwicklung kontinuierlich adressiert werden. Auf der Zeitachse von der Entwicklung bis zur Einführung entspricht das einem Linksrutsch – in Sicherheitskreisen «Shift Left» genannt.

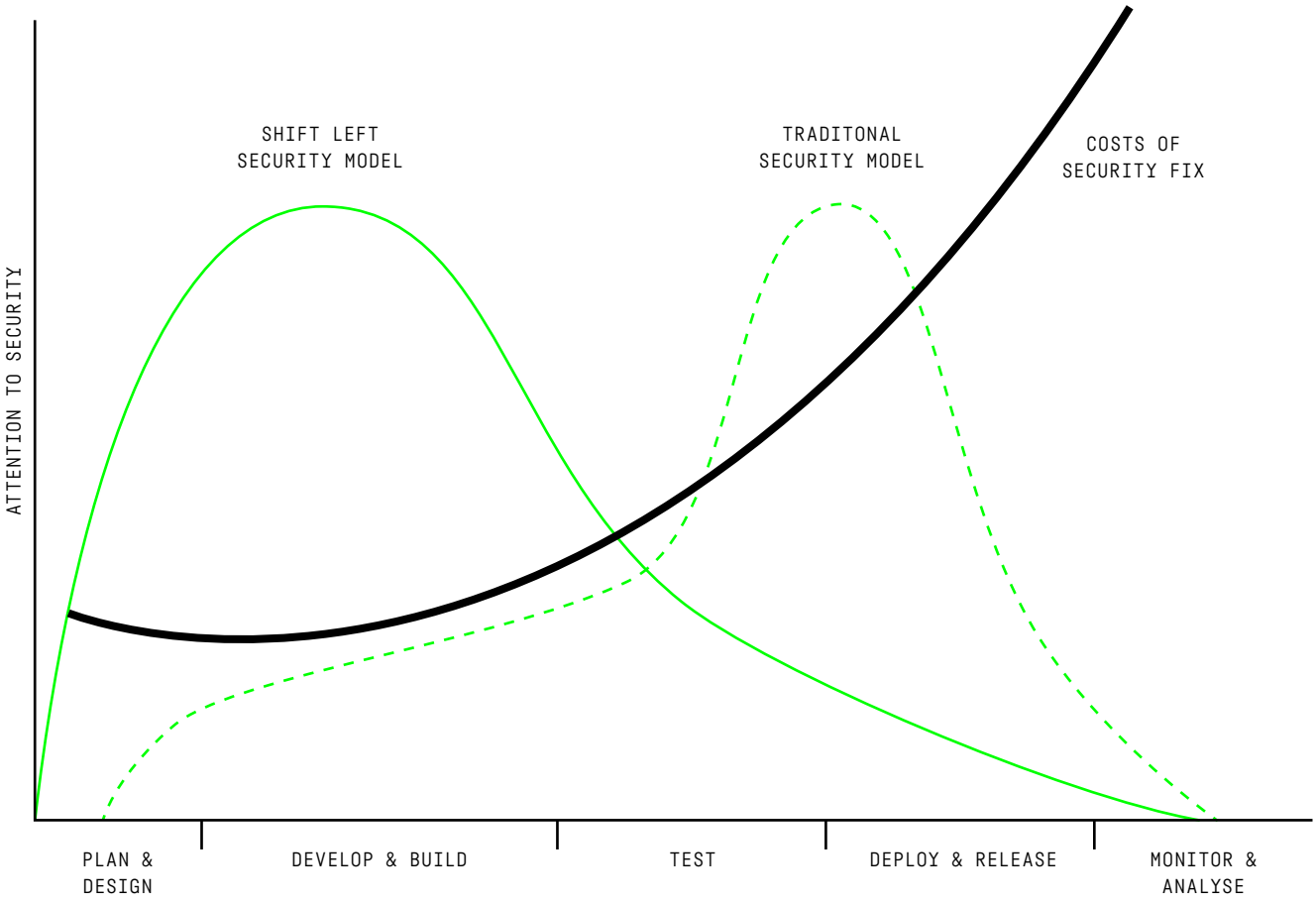
«Das Ziel ist es, Applikationen von Beginn an kontinuierlich zu schützen und dazu die Security nach vorne zu verlagern.»

_DANIEL ESTERMANN, PRODUCT MARKETING MANAGER AIRLOCK;
DANIEL.ESTERMANN@ERGON.CH

«Vereint und aligniert, erreichen Agile und DevSecOps ihr gemeinsames Ziel: die bestmögliche Kund:innenerfahrung und kurze Bereit-stellungszyklen.»

_ROMAN HUGELSHOFER, MANAGING DIRECTOR APPLICATION SECURITY,
MEMBER OF THE EXECUTIVE BOARD;
ROMAN.HUGELSHOFER@ERGON.CH

Shift Left:
Verlagerung der Sicherheit



Source: devopedia.org/shift-left

Automatisch sicher
DevSecOps integriert die Sicherheit von Applikationen nahtlos in Agile- und DevOps-Prozesse. Die Bereitstellung von sicherer Software wird durch den Einsatz von Security-Tools automatisiert, ohne den Software-Entwicklungszyklus zu verlangsamen. Sicherheitsprobleme bei Eigen- oder Fremdentwicklungen werden somit antizipiert, bevor sie auftreten. Zum Beispiel können mit einem Scanner Software-Bausteine bei jeder Änderung automatisch auf potenzielle Schwachstellen geprüft werden.

In der Regel ist es einfacher, schneller und kostengünstiger, Fehler sofort zu beheben, wenn sie auftreten. Und nicht erst in einem nachgelagerten Sicherheitstest oder kurz vor dem Go-live.

Je einfacher bedienbar, desto besser die Adaption
Trotz aller Vorsicht kann es jedoch vorkommen, dass Sicherheitslücken während der Laufzeit festgestellt werden. Besonders bei fremdentwickelten Anwendungen oder Open-Source-Komponenten besteht die Gefahr, dass Risiken auftauchen oder sich im Laufe der Zeit entwickeln. Das laufende Live-System muss folglich «geflickt» werden.

Security-Tools wie ein Microgateway, die bereits während der Entwicklung im Einsatz sind, erlauben es Entwickler:innen, nicht nur während des Baus der Applikation auf bequeme Weise Sicherheitsregeln selbst einzustellen, sondern auch wenn das System live ist. Und dies ohne dabei auf einen Sicherheitsprofi angewiesen zu sein. Dies ist wichtig, denn Sicherheitstools sind oftmals nicht für die einfache Bedienbarkeit durch die Entwickler:innen gemacht. Mit den richtigen Tools wird daher

Häufige Fehler bei der Umsetzung von DevSecOps

FEHLER	TIPP
ZU WENIG AUSDAUER	BEI ZU HOHEN ERWARTUNGEN BESTEHT DIE GEFAHR, ENTTÄUSCHT ZU WERDEN. DEVSECOPS IST EINE LANGE REISE, BEI DER ES KEINE ABKÜRZUNGEN GIBT.
TOP-DOWN-APPROACH	DEVSECOPS KANN NICHT EINFACH VOM MANAGEMENT VERORDNET WERDEN. WIE FÜR JEDE VERHALTENS- ODER BEWUSSTSEINSVERÄNDERUNG BRAUCHT ES STRUKTURELLE ANPASSUNGEN UND EIN KONTINUIERLICHES CHANGE MANAGEMENT, DAS INSBESONDERE AUCH KULTURELLE ASPEKTE VEREINT.
UNSTRUKTURIERTES VORGEHEN	ZUERST DIE RISIKEN IDENTIFIZIEREN, MASSNAHMEN PRIORISIEREN UND REALISTISCHE ZWISCHENZIELE SETZEN. IDEALER STARTPUNKT SIND PROBLEMBEREICHE UND ENGPÄSSE ZWISCHEN ENTWICKLUNG UND SECURITY. WASSERFALLARTIGE SICHERHEITSPROZESSE GILT ES, WO IMMER MÖGLICH, ZU ELIMINIEREN.
NUTZEN VON DEVSECOPS WIRD NICHT ANERKANNT	DIE VERWENDUNG VON STORYTELLING UND JEDE VERBESSERUNG IN FORM EINER SECURITY STORY IN DEN BACKLOG EINFLIESSEN LASSEN, ANALOG ZU USER STORIES. SO WIRD DIE UMSETZUNG PLANBAR UND VOR ALLEM FÜR ALLE STAKEHOLDER SICHTBAR. DAS SCHAFFT TRANSPARENZ UND VERTRAUEN. AUCH DIE DOKUMENTATION VON ROLLENÄNDERUNGEN UND DAS FESTHALTEN DER GEGENSEITIGEN ERWARTUNGEN IST FÜR EINE KLARE KOMMUNIKATION ZENTRAL, DAMIT DAS TEAM SEINE VERANTWORTUNG VERSTEHT.
SCHLECHT AUTOMATISIERBARE SICHERHEITSTOOLS	SICHERSTELLEN, DASS ALLE PARTEIEN DIE NOTWENDIGEN WERKZEUGE HABEN, UM DIE ARBEIT ZU ERLEDIGEN. AUCH BEI SECURITY-TOOLS GEWINNT DIE AUTOMATISIERUNG IMMER MEHR AN GEWICHT: DIE STEUERUNG ERFOLGT PER SKRIPT ODER API. GRAFISCHE BENUTZER:INNENOBERFLÄCHEN KÖNNEN DEN EINSTIEG ERLEICHTERN, EIGNEN SICH ABER SCHLECHT FÜR DIE AUTOMATISIERUNG.
ALLEINIGER FOKUS AUF CODE-ANALYSE	MIT APPLICATION SECURITY TESTING LASSEN SICH BEKANNTE ANGRIFFSVEKTOREN UND SCHWACHSTELLEN FRÜH ERKENNEN. UM AUCH NEUARTIGE ODER SOGAR UNBEKANNTE ANGRIFFE ZU VERHINDERN, SIND MODERNE WEB APPLICATION FIREWALLS ALS ZUSÄTZLICHER SCHUTZ NACH WIE VOR PFLICHT. IN DEVSECOPS-ARCHITEKTUREN WIRD DIESE FUNKTION VERMEHRT VON MICROGATEWAYS ÜBERNOMMEN [Z.B. AIRLOCK MICROGATEWAY]. DEREN SICHERHEITSMODELL GARANTIERT, DASS NUR SOLCHE AUFRUFE DIE ANWENDUNG ERREICHEN, DIE DIE ENTWICKLER:INNEN EXPLIZIT ALS GÜLTIG TAXIERT HABEN.

das Sicherheitsbewusstsein aller gefördert und somit zum integralen Teil der Software-Entwicklung. Da die Budgets für Security-Tools vielfach von den Security-Teams gesprochen werden, ist die einfache Bedienbarkeit für Entwickler:innen ein wichtiger Erfolgsfaktor in der Adaption.

Doppelter Schutz, doppelte Sicherheit

Durch den DevSecOps-Ansatz wird die Sicherheit in Applikationen optimal integriert. Es wird garantiert, dass die Cybersecurity mit der Innovationsgeschwindigkeit Schritt halten kann, und es beginnt der Aufbau einer Kultur und Zusammenarbeit zwischen Entwicklungs-, Sicherheits- und Betriebsteams. Auf Unternehmensebene ist es jedoch unmöglich, Sicherheit flächendeckend anzuwenden, da es ältere, nicht unterstützte Legacy-Systeme, Software-Bausteine von Drittanbietern oder losgelöste Aktivitäten anderer Abteilungen gibt, die möglicherweise ausserhalb des Zuständigkeitsbereichs der Entwicklungsteams liegen.

Solange Legacy-Applikationen ausserhalb der DevSecOps-Umgebung existieren – oder DevOps-Teams die Sicherheit nicht vollständig von Grund auf implementieren –, sind herkömmliche Tools wie zum Beispiel eine Firewall zum doppelten Schutz von Applikationen und zur Abschwächung von Angriffen nach wie vor empfohlen.

Der Ansatz für einen doppelten Schutz ist weit verbreitet, da diese Ausgangslage heute in den meisten modernen Organisationen gegeben ist; insbesondere bei Bewegungen wie Open Banking, bei denen Banken mit etablierten Legacy-Umgebungen auf eine schnelle und sichere Einbindung von Drittanwendungen angewiesen sind. Wichtig ist, dass solche Massnahmen schon als Teil des Lebenszyklus der Software-Entwicklung eingeplant werden. So wird bei der Entwicklung der Applikation sichergestellt, dass die Regeln für den Schutz auch den Anforderungen der Benutzer:innen entsprechen. Der Schutz soll höchstmöglich, nicht spürbar und nicht einschränkend sein.

Kosten sparen durch Automatisierung

Der initiale Aufwand für diese Automatisierung der Sicherheit ist nicht zu unterschätzen. Jede bedeutende Veränderung verlangsamt vorerst das Tagesgeschäft und zieht in der direkten Konsequenz Kosten nach sich.

Doch die Investition lohnt sich: Aufwendige manuelle Checks und damit verbundene Fehlerquoten werden reduziert und sowohl Sicherheit als auch Geschwindigkeit erhöht.

Zweifellos ist es finanziell von langfristigem Vorteil, erhebliche Sicherheitsvorfälle und daraus resultierende Imageschäden zu verhindern, bevor sie auftreten. Die Fähigkeit, einen Angriff zu erkennen und schnell handeln zu können, ist zentral. Zudem schafft DevSecOps ein agileres System, das schneller gestartet und aktualisiert werden kann. Unter Einbezug von DevSecOps-Engineers können Unternehmen ihre Sicherheitsinfrastruktur automatisieren und damit einen zeitaufwendigen, hochtechnischen und fehleranfälligen Prozess vereinfachen.

Menschen, Prozesse und Tools

Das Trio Menschen, Prozesse und Tools spielt eine wichtige Rolle für den Erfolg von DevSecOps. Es braucht eine Kultur, die erkennt, dass es kein «wir» und «die», sondern nur ein «wir» gibt. Alle sind gemeinsam für die Sicherheit der Software verantwortlich. Was einfach klingt, erfordert einen komplett neuen Denkansatz.

Das Security-Team muss glauben, dass Entwickler:innen und DevOps-Expert:innen sichere Software schreiben und bereitstellen wollen. Die DevOps-Teams müssen wiederum erkennen, dass die Sicherheitsprofis nicht diejenigen sind, die einfach «Nein» sagen und Innovation bremsen. Stattdessen sind sie damit beauftragt, Unternehmen vor Sicherheitsangriffen zu schützen, und agieren als Coaches, indem sie Entwicklungsteams beim Aufsetzen von automatisierten Sicherheitschecks unterstützen. So werden Entwickler:innen im sicheren Programmieren geschult und auf jegliche Angriffsszenarien sensibilisiert. Solche neuen Denkansätze zu vereinen, macht Arbeit und erfordert Zeit und einen kulturellen Wandel.

Weiter gilt es zu beachten, dass gekaufte Security-Tools normalerweise vom Security-Team und -Budget bereitgestellt und genehmigt werden. Wenn die gekauften Tools nun im DevSecOps-Prozess integriert sein sollen, müssen sie nicht nur hohe Sicherheitsanforderungen erfüllen, sondern auch hinsichtlich Benutzer:innenfreundlichkeit optimiert und auf die Bedürfnisse der Entwickler:innen und DevOps-Engineers zugeschnitten sein. Sicherheitsanbieter, die DevSecOps fördern wollen, müssen sich dieser Anforderungen bewusst sein.

Gekommen, um zu bleiben

DevSecOps gilt heute als moderne Art der Produktentwicklung. Die Adaption ist noch zögerlich, doch die Zukunft gehört letztendlich immer den Mutigen.

Die zwei grössten Vorteile sind Geschwindigkeit und Sicherheit. Entwicklungsteams liefern besseren, sichereren Code, und das auch noch schneller und damit kostengünstiger. DevSecOps macht das Thema Security zur gemeinsamen Verantwortung von Entwicklungs-, Sicherheits- und Betriebsteams. «Dank den richtigen Tools und gemeinsamem Nutzer:innenfokus wird Software sicherer und schneller», so das DevSecOps-Motto.

Dieses Umdenken kann Security vom Bremser zum Beschleuniger wandeln. Voraussetzung für die erfolgreiche Einführung von DevSecOps ist das Bewusstsein aller Beteiligten, dass so ein Projekt mehrere Unternehmensbereiche betrifft.

Mit der Verlagerung der Security nach links steigern Unternehmen also nicht nur ihre digitale Handlungsfähigkeit, sondern rüsten sich für eine digitale Zukunft auf der Überholspur. />