Berliner Hochschule für Technik

Fachbereich VI - Informatik und Medien
Studiengang IT-Sicherheit Online / Medieninformatik

Vorbereitung 11 - 13

PARETO CONSULTING

Modul:	Sicherheitsmanagement
Dozent:	Sven Zehl
vorgelegt von:	Gruppe 1 Christine Kuczera Dirk Drutschmann Hicham Naoufal Michael Schröter Jan Zimmermann Ivo Valls

Bedrohungsmodelierung und Entwicklung - Vorbereitung

a) Kennen Sie aus eigener Erfahrung Projekte, die budgettechnisch und zeitlich im Plan geblieben sind?

In meiner Projektarbeit bei Bayer (vor 10 Jahren) habe ich an dem Relaunch für das Thrombosemittel "Xarelto" mitgewirkt. Das Projekt umfasste umfangreiche Änderungen an der Benutzeroberfläche (UI) und

eine vollständige Neugestaltung der Projektstruktur. Das Gesamtbudget für dieses Projekt betrug ca. 500.000 Euro und die Zeitachse war auf sechs Monate festgelegt.

Die Herausforderung in diesem Projekt bestand nicht nur darin, eine intuitivere und benutzerfreundlichere Oberfläche zu erstellen, sondern auch sicherzustellen, dass alle Projektphasen ordnungsgemäß koordiniert und ausgeführt wurden. Dies war das erste Mal, dass das Unternehmen die agile Methodik Scrum in einem Projekt implementierte. Obwohl es anfängliche Bedenken gab, erwies sich diese Entscheidung als äußerst vorteilhaft.

Scrum half dabei, die Projektaufgaben in kleinere, handhabbare Arbeitspakete zu unterteilen, die von verschiedenen Teams innerhalb bestimmter Zeitrahmen, sogenannten Sprints, bearbeitet wurden. Diese Methode ermöglichte es, den Fortschritt regelmäßig zu überprüfen und schnelle Anpassungen an unerwartete Änderungen oder Herausforderungen vorzunehmen.

Kommunikation und Transparenz waren in diesem Prozess entscheidend. Regelmäßige Stand-up-Meetings und der Einsatz von Scrum-Boards förderten die Zusammenarbeit und hielten alle auf dem neuesten Stand des Projektfortschritts. Zusätzlich wurde eine effektive Risikomanagementstrategie implementiert, um potenzielle Hindernisse frühzeitig zu erkennen und zu mindern.

b) Recherchieren Sie zum Sicherheitsvorfall Maersk 2017, als über die Buchhaltungssoftware Schadsoftware eingeschleust wurde. Wie hatte Maersk reagiert?

Der Vorfall mit Maersk im Jahr 2017 war Teil einer größeren Cyberattacke namens "NotPetya". Es handelte sich um eine raffinierte Ransomware-Attacke, die sich über eine ukrainische Buchhaltungssoftware verbreitete. Nachdem die Schadsoftware in das Maersk-System eingedrungen war, verursachte sie erhebliche Schäden, indem sie Daten auf den infizierten Systemen verschlüsselte. Maersk reagierte, indem es seine IT-Systeme abschaltete, um die Ausbreitung des Angriffs zu verhindern. Dies führte zu erheblichen Unterbrechungen im Betriebsablauf. Maersk arbeitete intensiv an der Wiederherstellung seiner Systeme und Kommunikationsnetzwerke und nahm dabei auch externe Hilfe in Anspruch. Währenddessen wurden die arbeiten analog weitergeführt, was weitreichende Folgen nach sich zog bis hin zum Einfluss auf die Weltwirtschaft. Diese Ereignisse unterstreichen die Bedeutung einer robusten Cybersicherheitsstrategie und einer effektiven Reaktionsplanung im Falle von Sicherheitsvorfällen.

Quelle 1: https://www.heise.de/news/Cyber-Attacke-NotPetya-Unternehmen-haben-immer-noch-viel-Arbeit-mit-dem-Fallout-des-Angriffs-3782794.html

Quelle 2: https://www.heise.de/news/Alles-was-wir-bisher-ueber-den-Petya-NotPetya-Ausbruch-wissen-3757607.html

c)

Der Heise-Verlag entschied sich nach einer Attacke von Verschlüsselungssoftware im Frühjahr 2021 für eine Full-Disclosure-Strategie. Die Full-Disclosure-Strategie besteht darin, alle Details eines Sicherheitsvorfalls offen zu legen. Dies kann dazu beitragen, das Vertrauen in die Organisation zu stärken, indem transparente Kommunikation und Verantwortungsbewusstsein gezeigt wird. Außerdem ermöglicht es anderen Unternehmen, von dem Vorfall zu lernen und ihre eigenen Sicherheitsmaßnahmen zu

verbessern. Es ist jedoch wichtig zu beachten, dass diese Strategie auch Risiken birgt, da sie Informationen offenlegen kann, die von böswilligen Akteuren ausgenutzt werden könnten. Die Entscheidung für eine solche Strategie hängt daher von vielen Faktoren ab, darunter die Art des Vorfalls, die potenziellen Auswirkungen auf Kunden und andere Stakeholder und die allgemeine Unternehmenspolitik in Bezug auf Transparenz und Offenheit.