Evaluation von Qubes OS für den Einsatz in klein- und mittelständischen Software-Entwicklungsunternehmen

Tobias Schotter
Medieninformatik
Ostbayerische Technische Hochschule Amberg-Weiden
Amberg, Germany
Email: tobias.schotter@example.com

***Abstract*—Hardly any company in Germany is spared from an increasing number of cyber-attacks. Cybercrime offences now cause damage of around 220 billion euros per year in Germany alone. The Qubes OS operating system offers an approach to protect computers further than conventional IT security measures by isolating processes, applications, and hardware through compartmentalization, for example in the form of virtual machines. Qubes follows the practical approach of limiting and containing damage to separate valuable data from risky activities.**

In the context of this thesis, concepts are evaluated on how small and medium-sized software development companies can integrate Qubes OS into their everyday use. Typical usage scenarios of software engineers are examined and compared with a native Windows 10 operating system. Based on the evaluations, the necessary changes in the everyday cycle of a software developer are presented and compared with the known "best practices".

I. Einleitung

Heutige IT-Systeme sind einer Vielzahl von Angriffen ausgesetzt, sowohl Firmencomputer als auch private Systeme sind betroffen. Anti-Viren-Software und Firewalls sind typische Gegenmaßnahmen, jedoch verschaffen sich Angreifer immer wieder Zugang zu Unternehmenssystemen und verursachen erhebliche Schäden. Allein in Deutschland belaufen sich die geschätzten Schäden durch Cyberkriminalität auf circa 220 Milliarden Euro pro Jahr [**?**].

Qubes OS stellt ein Open-Source-Betriebssystem dar, das durch die Isolation von Prozessen, Anwendungen und Hardware ein hohes Maß an Sicherheit bietet. Anwendungen werden in separaten und teilweise temporären virtuellen Maschinen (VMs) ausgeführt, wodurch die Angriffsoberfläche verringert wird. Diese Arbeit untersucht, wie Qubes OS in klein- und mittelständischen Software-Entwicklungsunternehmen sinnvoll eingesetzt werden kann.

II. Methodik

Die Methodik dieser Arbeit besteht aus einer Evaluation der Nutzung von Qubes OS in einem realistischen Szenario von kleinen und mittleren Softwareunternehmen. Dazu werden typische Nutzungsszenarien für Software-Ingenieure untersucht und mit der Nutzung eines nativen Windows 10 Betriebssystems verglichen. Es wird eine Gegenüberstellung von Sicherheitsmechanismen herkömmlicher IT-Sicherheitsmaßnahmen und den spezifischen Mechanismen von Qubes OS vorgenommen.

III. Informationssicherheit

A. Relevanz von Informationssicherheit

Die meistgenutzten Betriebssysteme wie Windows und macOS sind zwar beliebt aufgrund ihrer Benutzerfreundlichkeit, weisen jedoch erhebliche Sicherheitsprobleme auf. Malware kann über E-Mails oder Websites in Systeme eindringen und dabei sensible Informationen gefährden. Es ist daher wichtig, alternative Sicherheitslösungen wie Qubes OS zu betrachten, das durch die Isolation von Prozessen eine hohe Sicherheit bietet.

B. Sicherheitsmechanismen von Qubes OS

Qubes OS verfolgt den Ansatz der Kompartimentierung, bei dem verschiedene Tätigkeiten in isolierten virtuellen Maschinen, den sogenannten Qubes, getrennt werden. Dies bedeutet, dass eine kompromittierte VM keine anderen VMs beeinträchtigen kann. Beispielsweise können Weblinks in sogenannten DisposableVMs, die sich nach Beendigung selbst zerstören, geöffnet werden, wodurch die Gefahr einer Infektion des Gesamtsystems minimiert wird.

IV. Analyse von Nutzungsszenarien

A. Administrative Nutzungsszenarien

Die Installation von Qubes OS erfordert spezifische Hardwareanforderungen und die Aktivierung von IOMMU-basierter Virtualisierung. Software kann über TemplateVMs installiert und auf mehrere AppVMs verteilt werden, wodurch eine effiziente Administration ermöglicht wird. Ein weiteres Nutzungsszenario ist die Installation einer Windows-VM innerhalb von Qubes OS, um Windows-spezifische Anwendungen auszuführen.

B. Entwicklungsprozesse

Qubes OS kann ebenfalls für Entwicklungsprozesse genutzt werden. Es wurden verschiedene Server-Backend-Technologien wie Node.js, Java und ASP.NET Core unter Qubes OS getestet. Die Ergebnisse zeigen, dass diese Technologien lauffähig sind und Entwicklungsprozesse sicher durchgeführt werden können.

V. Fazit und Ausblick

Die Evaluation von Qubes OS zeigt, dass das Betriebssystem ein hohes Maß an Sicherheit bietet, insbesondere durch die Isolation von Anwendungen in separaten VMs. Für kleine und mittelständische Softwareunternehmen stellt dies eine vielversprechende Alternative zu herkömmlichen Sicherheitslösungen dar. Zukünftige Arbeiten könnten sich auf die Optimierung der Benutzerfreundlichkeit und die Integration weiterer Sicherheitswerkzeuge konzentrieren.

References