GITSA

Gamified IT-Security Awareness

Programm / Ausschreibung	Kooperationsstrukturen, Kooperationsstrukturen, FH - Forschung für die Wirtschaft (COIN-Aufbau) Ausschreibung 2022	**Status**	laufend
Projektstart	01.05.2023	**Projektende**	30.04.2027
Zeitraum	2023 - 2027	**Projektlaufzeit**	48 Monate
Keywords	IT-Security; Awarenesschulung; Gamification		

Projektbeschreibung

Immer noch ist der Mensch die zugrundeliegende Ursache für die meisten erfolgreichen Angriffe auf IT-Infrastruktur in Unternehmen; 91% der erfolgreichen Angriffe über das Internet beginnen bei den Mitarbeiter*innen. In der überwiegenden Anzahl der Fälle geschieht dies auch im besten Glauben und Vertrauen der betroffenen Mitarbeiter*innen, ohne dem Unternehmen bewusst schaden zu wollen.
Abseits technischer Maßnahmen kann man diesem Problem nur durch Schulungen/awarenessbildende Maßnahmen begegnen, wobei verpflichtende regelmäßige Trainings zur IT Sicherheit in vielen Unternehmen bereits gut etabliert sind. Diese Trainings werden allerdings häufig von den Mitarbeiter*innen eher als lästige Pflichtübung denn als wichtiger Pfeiler der IT-Security Strategie wahrgenommen.
Bereits in der Vergangenheit gestaltete das IT-Security Kompetenzzentrum eine Awarenessmaßnahme in Form eines „Capture-the-Flag“-ähnlichen Wettbewerbs für Mitarbeiter*innen eines Finanzdienstleisters. Die Teilnehmer*innen mussten auf einer selbst entwickelten Onlineplattform kleine IT-Security Challenges lösen, mit dem Ziel, damit die eigene Awareness zu erhöhen und die Anfälligkeit für Phishingmails und ähnliche Angriffe spielerisch zu senken. Insbesondere durch die aktive Beschäftigung mit den vermittelten Thematiken verfestigen sich die Themen deutlich besser als durch rein passives „Durchklicken“.
Die wesentlichen Erkenntnisse aus diesem Projekt waren, dass die Plattform gut angenommen wird und auch in anderen Unternehmen Bedarf besteht; die Entwicklung dieser erfordert allerdings mehr Ressourcen als vorhanden, sowie den Aufbau zusätzlichen Know-Hows. Mehrmandantenfähigkeit, einfaches Deployment, gute Skalierbarkeit, ständige Fort- und Neuentwicklung von Challenges sowie die Entwicklung konkreter Messbarkeitskriterien erwiesen sich ohne explizites Förderprojekt als nicht effektiv bewältigbare Herausforderungen.
Die Ziele dieses F&E-Projekts sind nun u.a.:
1) Strukturierte Erhebung und Klassifizierung der häufigsten Anwender*innenfehler, die zu IT-Security-kritischen Vorfällen geführt haben
2) Konzept und Entwicklung einer generischen, erweiterbaren und schnell deploybaren Plattform unter Verwendung aktueller Technologien für die Abhaltung von Awarenessschulungen für unterschiedliche Zielgruppen
3) Konzept, Entwicklung, Deployment und praktische Evaluierung von entsprechenden Challenges unter Berücksichtigung

der gewonnenen Erkenntnisse aus Ziel 1, bei bereits existierenden bzw. noch zu akquirierenden Partner*innen
4) Evaluierung, inwieweit eine solche Plattform auch in der Lehre (Master IT-Security, Bachelor Computer Science, ...) unterstützen kann, insbesondere auch im Hinblick auf den anhaltenden Trend zum Remote Unterricht (Beispielsweise für Aufgaben im Bereich Ethical Hacking/Penetration Testing)
5) Entwicklung und Evaluation von Messkriterien, um die Schulungseffektivität für Unternehmen sichtbar zu machen

Abstract

Humans are still the underlying cause of most successful attacks on corporate IT infrastructure; 91% of successful attacks via the Internet start with employees. In the vast majority of cases, this happens in the best belief and trust of the affected employees, without consciously wanting to harm the company.
Apart from technical measures, this problem can only be countered through training/awareness-building measures, whereby mandatory regular training on IT security is already well established in many companies. However, these trainings are often perceived by employees more as an annoying compulsory exercise than as an important pillar of the IT security strategy.
In the past, the IT Security Competence Center organized an awareness measure in the form of a "capture-the-flag"-like competition for employees of a financial service provider. The participants had to solve small IT security challenges on a self-developed online platform with the aim of increasing their own awareness and reducing their susceptibility to phishing emails and similar attacks in a playful way. In particular, active engagement with the topics taught is much more effective than purely passive "clicking through".
The main findings from this project were that the platform is well received and that there is also a need for it in other companies; however, developing it requires more resources than are available, as well as building up additional expertise. Multi-tenancy, ease of deployment, good scalability, continuous development of challenges, and the development of concrete measurability criteria proved to be challenges that could not be effectively met without an explicit funding project.
The goals of this R&D project now include:
1) Structured survey and classification of the most common user errors that led to IT security-critical incidents.
2) Design and development of a generic, extensible and rapidly deployable platform using current technologies for delivering awareness training to different target groups.
3) Concept, development, deployment and practical evaluation of corresponding challenges, taking into account the knowledge gained from objective 1, with existing and partners yet to be acquired partners.
4) Evaluation of the extent to which such a platform can also support teaching (Master IT-Security, Bachelor Computer Science, ...), especially with regard to the continuing trend towards remote teaching (e.g. for tasks in the area of ethical hacking/penetration testing).
5) Development and evaluation of measurement criteria to make training effectiveness visible for companies.

Projektpartner

- FH Campus Wien Forschungs- und Entwicklungs GmbH