ALARM
Awareness Labor KMU Informationssicherheit

Niederschwelliges Sicherheitskonzept zum Thema Tailgating

für Geschäftsführung und IT-Verantwortliche

Thinking Objects GmbH

Stand: Mai 2023

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Das vorliegende **niederschwellige Sicherheitskonzept für KMU** ist eines von insgesamt sieben Sicherheitskonzepten, die im dreijährigen Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ der Technischen Hochschule (TH) Wildau verfasst werden.

Das Projekt „ALARM Informationssicherheit“ wird vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördert.

Projektlaufzeit

01.10.2020 – 30.09.2023

Das niederschwellige Sicherheitskonzept für KMU basiert auf Ergebnissen der im Projekt „ALARM Informationssicherheit“ durch den Unterauftragnehmer Thinking Objects (TO) GmbH in Pilotunternehmen durchgeführten „Vor-Ort-Angriffen“.

Das diesem Sicherheitskonzept zugrundeliegende Vorhaben wird mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz unter dem Förderkennzeichen 01MS19002A gefördert.

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren*, der Initiative *IT-Sicherheit in der Wirtschaft* und *Digital Jetzt* umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.it-sicherheit-in-der-wirtschaft.de.

Inhaltsverzeichnis

1 Einleitung **3**

2 Maßnahmen **4**

2.1 Zutrittskontrolle 4

2.2 Besuchsmanagement 4

2.3 Clean Desk und Clear Screen Policy 5

2.4 Räume mit sensiblen Geräten/Daten geschlossen halten 5

2.5 Meldeweg 5

2.6 Awareness 6

1 Einleitung

Was ist unter dem Begriff **Tailgating i**m Kontext der Informationssicherheit zu verstehen?

Tailgating kann frei mit „Durschlüpfen“ übersetzt werden. Es handelt sich um eine Form eines Angriffes, der dem Überbegriff Social Engineering zugeordnet wird . Kriminelle schaffen sich dabei unbefugt Zugang zum Unternehmen. Dabei zielt dieser Angriff auf die Beschaffung von sensiblen Informationen, Manipulation von Geräten oder Mitnahme ab. Diese Aktionen können für weitere Angriffe genutzt werden. U.a. Erpressungen mit der Drohung, die entwendeten/kopierten sensiblen Daten zu veröffentlichen oder durch die manipulierten Geräte und Systeme unbrauchbar zu machen.

Eine klassische Form des Tailgatings ist es, den Zugang zu einem nicht öffentlichen Bereich im Unternehmen dadurch zu erlangen, dass die Kriminellen mit einer berechtigten Person durch die noch offene Tür „durchschlüpfen“.

Dabei nutzen die Kriminellen häufig die Gutmütigkeit und Hilfsbereitschaft von Beschäftigten aus:

- Eine hilfesuchende Person steht vor der zugangsgesicherten Tür und spricht Sie an: „Ich habe meinen Schlüssel/Zugangskarte vergessen, können Sie mich mit reinlassen?“
- Jemand ist mit Unterlagen oder Paketen voll beladen, damit Sie ihr die Tür aufhalten.
- Eine Person „vom Fach“, also in entsprechend typischer Arbeitskleidung, das kann der Blaumann oder das Business Outfit sein, geht wie selbstverständlich mit Ihnen durch Tür.

Hier sind noch viele weitere Szenarien denkbar, die auf ein „normales“ soziales Verhalten abzielen, um damit unberechtigt Zugang zu erhalten.

2 Maßnahmen

Es gibt einige Maßnahmen, die es Kriminellen erschweren, einen solchen Angriff erfolgreich durchzuführen. Hiermit lassen sich die Auswirkungen und Schäden im Idealfall verhindern oder zumindest mindern.

2.1 Zutrittskontrolle

Neben den klassischen Maßnahmen zur Prävention von Einbrüchen, also z.B. physischen Barrieren wie Zäunen oder der Überwachung durch einen Sicherheitsdienst, sind weitere Maßnahmen möglich.

Je früher die Zutrittsberechtigung von Personen kontrolliert wird, umso geringer die Gefahr, dass Dritte sich unberechtigt Zutritt verschaffen. Zum Beispiel kann hinterfragt werden, ob tatsächlich eine „offene“ Lobby benötigt wird, die Werkstore immer offenstehen müssen oder die Getränkelieferung durch die immer offene Kellertür erfolgen muss.

Berechtigte Personen, das können auch Lieferanten (nach entsprechender Bewertung) sein, sollten den Zutritt durch Schlüssel oder auch elektronische Schließsysteme erhalten. Diese bieten den Vorteil, dass Zutrittsberechtigungen zu unterschiedlichen Bereichen (siehe unter Räume mit sensiblen Geräten/Daten geschlossen halten) nicht am physikalischen Schlüssel hängen und zum Beispiel bei Verlust oder Diebstahl schnell und mit geringen Kosten angepasst werden können, da nur einen Zugangstoken ersetzt werden muss, statt einen oder mehrerer Schließzylinder auszutauschen.

Auch Berechtigungen für Gäste (siehe unter Besuchsmanagement) können hiermit einfach verwaltet und i.d.R. zeitlich begrenzt werden.

2.2 Besuchsmanagement

Besuchende sollten in der Regel registriert werden, so dass ein Überblick über nicht firmenangehörige Personen besteht. In Bereichen, in den Publikumsverkehr besteht, ist dies selbstverständlich nicht sinnvoll. Hier ist darauf zu achten, dass der Zugang zu nicht öffentlichen Bereichen gesichert ist.

Die Ausgabe von Ausweisen für Besuchende erleichtert es den Beschäftigten, diese zu erkennen und auf deren Verhalten besonders zu achten. Verstärkt wird dieser Effekt durch anders aussehende Kennzeichnungen für die eigenen Beschäftigten.

Eine klare Regelung und Kommunikation im Unternehmen, wie mit Dritten, ggf. auch nur in bestimmten Bereichen, umgegangen werden soll, hilft es den Beschäftigten, diese Regelungen zu verinnerlichen und umzusetzen.

Hierzu gehört auch die Regelung, ob Besuchende immer zu begleiten sind. Dies kann je nach Branche und Gegebenheit bereits aus arbeitssicherheitsrechtlichen Gründen gegeben sein.

Es ist wichtig, dass die bestehenden Regelungen bekannt sind, dem Schutzbedarf Rechnung tragen und von allen Personen im Unternehmen, insbesondere auch der Leitungsebene, beachtet und gelebt werden.

2.3 Clean Desk und Clear Screen Policy

Die Clean Desk und Clear Screen Policy, auf Deutsch sinngemäß aufgeräumter Schreibtisch und leerer Bildschirm, haben nicht primär eine ordentliche Arbeitsumgebung als Ziel – auch wenn das ein positiver Nebeneffekt sein kann. Hierbei geht es um den Schutz sensibler Daten, die durch Unbefugte, sowohl intern als auch extern, nicht eingesehen werden dürfen.

Es sollten also keine Dokumente mit vertraulichen Daten, das können sowohl personenbezogene Daten, aber auch vertrauliche Geschäftsdaten sein, offen herumliegen, wenn nicht aktiv mit diesen gearbeitet wird.

Auch sollte der Zugriff auf den elektronischen Arbeitsplatz bei Abwesenheit durch Dritte nicht möglich sein. Clear Screen umfasst somit sowohl, dass auf dem Bildschirm keine vertraulichen Informationen zu sehen sind, als auch dass der Arbeitsplatz beim Verlassen gesperrt wird. Je nach Branche und Bereich können auch schon Namen von Dateien sensible Informationen enthalten, beispielweise „Kündigung Herr Mustermann“ oder „Übernahmen der Musterfirma AG“.

Hat sich jemand mittels Tailgating Zugang verschafft, können solche Informationen leicht ausgespäht, kopiert oder entwendet werden. Auch der nur kurze Zugriff auf den entsperrten Arbeitsplatz ermöglicht es Kriminellen, Informationen abzuziehen oder Schadsoftware zu installieren. Ebenso ist ein Identitätsmissbrauch denkbar, indem beleidigende oder sonst kompromittierende Nachrichten verschickt werden. Insbesondere bei externen Adressaten ist der Schaden nur sehr aufwändig wieder zu beheben.

Beide Themen sollten durch entsprechende Richtlinien/Anweisungen organisatorisch geregelt sein, die sich am Arbeitsalltag und dem Schutzbedarf orientieren. Die Clear Screen Vorgabe kann durch technische Maßnahmen, z.B. dem automatisierten Sperren nach Zeit, unterstütz werden. Eine allgemeingültige Zeitvorgabe gibt es nicht, auch diese muss sich am Arbeitsalltag und dem Schutzbedarf orientieren – das Terminal, auf dem ausschließlich der Kantinenplan läuft, darf gerne dauerhaft entsperrt bleiben, der Rechner mit Zugriff auf das Geheimrezept nicht.

2.4 Räume mit sensiblen Geräten/Daten geschlossen halten

Räume, in denen der Zugriff auf sensible Daten möglich ist, sollten nach Möglichkeit immer verschlossen sein, wenn sich niemand darin aufhält. Hier bieten sich verschiedene (Sicherheits-)Bereiche an, die je nach Schutzbedarf mit einer Zugangssicherung versehen sind und nur berechtigte Personen zulassen. Beispiele für solche Bereich wären das Firmengelände mit großzügigem Zugang, Gebäude nur noch für Beschäftigte, Flure nur nach Zugehörigkeit zu dem dort angesiedelten Bereich oder dem berechtigten Auftrag und Büros/Räume nur personalisiert.

2.5 Meldeweg

Es ist wichtig, einen Meldeweg für sicherheitsrelevante Ereignisse festzulegen. Für die Beschäftigten muss dieser Weg bekannt und eindeutig sein, damit er im Rahmen von Schulungen und Sensibilisierungsmaßnahmen (siehe Awareness) vermittelt und gelebt werden kann. Dabei ist auch das richtige Verhalten gegenüber einer unberechtigten Person mit aufzunehmen, welches stark vom jeweiligen Umfeld abhängig ist und von beobachten bis zu festhalten gehen kann.

2.6 Awareness

Es ist wichtig, dass die Beschäftigten für die Gefahren und Risiken sensibilisiert sind, die durch den unbefugten Zugang von Dritten entstehen. Eine klar kommunizierte Verfahrensweise für den Aufenthalt von Dritten innerhalb der Firma hilft, entsprechende Umgangsformen damit zu etablieren.

Wenn zum Beispiel allen klar ist, dass das Betreten der Firma nur nach Anmeldung erlaubt ist, können Beschäftigte besser dafür sensibilisiert werden, niemanden einfach so Zutritt zu gewähren oder gar wie oben beschrieben die Tür aufzuhalten.

Meldungen (siehe unter Meldeweg) sollten immer ernst genommen werden. Eine gute Kommunikation über anstehende Besuche, z.B. Reparaturarbeiten o.ä., hilft, keine Fülle von Fehlalarmen zu erhalten. Wie sensibel bzw. niederschwellig die Meldungen sein sollen, gilt es am eigenen Schutzbedarf zu orientieren und die Beschäftigten entsprechend zu informieren, was gemeldet werden soll und was nicht.

Technische Hochschule Wildau
Technical University of Applied Sciences

Thinking Objects

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

Tel. +49 711 88770400
Fax. +49 711 88770449
www.to.com