ALARM
Awareness Labor KMU Informationssicherheit

INFOBLATT – Security kompakt zum Thema Hacking

für Endanwender:innen

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 **INFOBLATT – Security kompakt 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 INFOBLATT – Security kompakt 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 Hacking – Wie kann ich mich schützen?

Sensibel mit eigenen Identitätsdaten umgehen.

Alles, was Sie dazu wissen müssen, finden Sie kurz und kompakt in diesem Infoblatt.

1.1 WARUM sind wir verantwortlich für unsere eigene Sicherheit?

IT-Sicherheitsbewusstsein (IT Security Awareness) ist von entscheidender Bedeutung, weil die Sicherheit einer Organisation oder einer Einzelperson in hohem Maße von den Handlungen und Entscheidungen ihrer Benutzer:innen abhängt.

Das Bewusstsein für IT-Sicherheit hilft Ihnen, potenzielle Bedrohungen zu erkennen und angemessen darauf zu reagieren. Indem Sie sich weiterbilden, Phishing-E-Mails, betrügerische Websites, schädliche Anhänge und andere Angriffsmethoden im Bereich des Social Engineerings zu erkennen, können Sie dazu beitragen, Hacker-Angriffe zu verhindern.

1.2 WIE können Sie sich schützen?

- **Starke Passwörter und Zwei-Faktor-Authentifizierung verwenden:**

Schützen Sie ihre Konten mit starken Passwörtern und aktivieren Sie die Zwei-Faktor-Authentifizierung, wo immer möglich. Dadurch wird es schwieriger für Angreifer, auf Konten zuzugreifen, selbst wenn sie Ihre Passwörter kennen. Detailliertere Informationen finden Sie unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html (15.06.23).

- **Software und Betriebssysteme aktualisieren:**

Halten Sie Ihre Betriebssysteme, Apps und Antivirenprogramme auf dem neuesten Stand. Regelmäßige Updates enthalten häufig Patches und Sicherheitsverbesserungen, die Ihre Geräte vor bekannten Schwachstellen schützen.

- **Vorsicht beim Öffnen von E-Mails und Anhängen:**

Seien Sie vorsichtig beim Öffnen von E-Mails von unbekannten Absendern oder beim Herunterladen von Anhängen. Phishing E-Mails können dazu verwendet werden, Ihre Kontoinformationen zu stehlen oder schädliche Software auf Ihrem Gerät zu installieren. Weitere kompakte Informationen finden Sie in unseren Infoblättern -**Phishing- und -CEO Fraud**.

- **Firewall und Antivirensoftware verwenden:**

Installieren Sie eine zuverlässige Firewall und Antivirensoftware auf Ihren Geräten. Diese helfen dabei, verdächtige Aktivitäten zu erkennen und schädliche Software zu blockieren. Detailliertere Informationen finden Sie unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Virenschutz-Firewall/virenschutz-firewall_node.html (15.06.23).

- **Vorsicht bei öffentlichen WLAN-Netzwerken:**

Vermeiden Sie die Nutzung von öffentlichen WLAN-Netzwerken für vertrauliche Aktivitäten wie Online-Banking oder das Zugreifen auf persönliche Konten. Wenn Sie öffentliches WLAN verwenden müssen, verwenden Sie ein virtuelles privates Netzwerk (VPN), um Ihre Verbindung zu sichern. Weitere Informationen finden Sie unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/Virtual-Private-Networks-VPN/virtual-private-networks-vpn_node.html (15.06.23)

- **Datensicherung:**

Regelmäßige Backups Ihrer wichtigen Daten können hilfreich sein, falls Ihre Geräte gehackt oder kompromittiert werden. Speichern Sie Backups an einem sicheren Ort außerhalb Ihrer Geräte.

- **Gesunde Skepsis:**

Seien Sie immer skeptisch gegenüber unerwarteten Anfragen, insbesondere wenn Sie aufgefordert werden, sensible Informationen preiszugeben oder ungewöhnliche Aktionen durchzuführen. Vertrauen Sie nicht blindlings auf die Identität einer Person, nur weil sie behauptet, ein Mitarbeiter oder eine Mitarbeiterin einer Organisation zu sein.

- **Persönliche Informationen geheim halten:**

Geben Sie niemals vertrauliche Informationen wie Passwörter, Kreditkarteninformationen oder Sozialversicherungsnummern preis, es sei denn, Sie sind sich sicher, dass die Anfrage legitim ist.

3 FEHLERKULTUR – Hilfen für den Ernstfall…

Fehler passieren allen von uns!

Wichtig: Wenn Sie betroffen sind, finden sie auf diesen Seiten hilfreiche Tipps und Checklisten: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html#doc131400bodyText3 (15.06.23).

Weitere Informationen erhalten Sie auch in unseren digitalen Lernszenarios:

https://alarm.wildau.biz/#learningScenarios

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