issa | INTERNATIONALE VEREINIGUNG FÜR SOZIALE SICHERHEIT | IVSS

Sektion für Maschinen- und Systemsicherheit

Tür zu!

Hackerabwehr für Kleinbetriebe

Factsheet
№ 3

Ein Beispiel aus der Praxis

Das historische Restaurant „Zum Lamm“ mit 20 Mitarbeitern ist ein beliebtes Ausflugsziel. In den letzten 10 Tagen blieb das Restaurant geschlossen, da sein Online-Reservierungssystem, seine Computer und sein digitales Bestellsystem nicht mehr benutzt werden können. Eine IT-Vertragsfirma wurde hinzugezogen, die auch Fortschritte bei der Wiederherstellung des ursprünglichen Zustands macht, aber die Kosten sind hoch, und der Verdienstausfall während dieser 10 Tage noch deutlich höher.

Wie kam es dazu?

Einige Tage zuvor hatte der Eigentümer eine sehr echt wirkende E-Mail mit einer Rechnung erhalten, die vermeintlich von seinem vertrauenswürdigen Weinlieferanten stammte. Es stellte sich jedoch heraus, dass der Absender ein Cyberkrimineller war, der sich als Weinlieferant ausgab. Der Anhang war ein Computervirus, der schon begonnen hatte, Dateien zu verschlüsseln und Computersysteme zu deaktivieren, gefolgt von der Nachricht, dass die Störung dauerhaft sein würde, wenn kein Lösegeld von 30.000 Euro gezahlt würde.

Diese Geschichte klingt unglaubwürdig? Ähnliche Vorfälle kommen sehr oft vor!

Diese Art von Computerviren wird als „Ransomware“ bezeichnet. Wenn sie aktiviert wird, beginnt sie mit der Verschlüsselung der Dateien auf dem Computer. Dann ist ein Zugriff auf diese praktisch nicht mehr möglich, denn nur der Cyberkriminelle verfügt über den „digitalen Schlüssel“. Dies ist nur eine von verschiedenen Arten von Computerviren, die von Hackern verwendet werden.
Das alles klingt sehr technisch und beunruhigend. Die gute Nachricht ist: die wirksamste Verteidigung gegen solche Cyber-Bedrohungen ist eigentlich weder schwierig noch technisch anspruchsvoll. Die überwiegende Mehrheit der Cyberkriminellen ist auf das sogenannte „Social Engineering“, also die zwischenmenschliche Beeinflussung, angewiesen, bei der es darum geht, einen Menschen zu täuschen, damit er Fehler macht, und dem Cyberkriminellen Zugang zu seinem Computersystem ermöglicht. Dies kann eine E-Mail sein, die vorgibt, von einer Organisation zu stammen, der Sie vertrauen, wie z.B. Ihrer Bank oder einem Online-Shop.
Es könnte eine SMS mit der Aufforderung „Überprüfen Sie diesen Link“ sein, mit einem Link, in dem der Name eines Freundes genannt wird, so dass Ihr Mobiltelefon dies in Ihren bestehenden Chatverlauf mit ihm einfügt. Oder ein Screenshot eines Videos, das mit Ihnen geteilt wird und zu interessant aussieht, um es zu verpassen. Wenn Sie dann aufgefordert werden, ein spezielles Software-Update zu installieren, um es anzusehen, klicken Sie vielleicht darauf, weil die Neugierde zu groß ist. In allen Fällen will der Cyberkriminelle Sie dazu verleiten, einen Fehler zu machen, nämlich auf Ihrem Computer etwas zu installieren, was Ihnen schadet.

Grundlegende Cyber-Hygienemaßnahmen zum Schutz Ihres Unternehmens vor Social Engineering

Zu erkennen, dass man getäuscht worden ist, ist nie ein gutes Gefühl.

Außerdem glaubt jeder, dass er dafür zu klug ist. Die Realität sieht leider völlig anders aus. Sogar die erfahrensten Cyber-Sicherheitsexperten und Professoren sind schon getäuscht worden, und zwar in einigen Fällen bei sehr öffentlichkeitswirksamen Vorfällen. Wir alle sind anfällig für Täuschungen. Einer der wichtigsten Gründe dafür ist, dass eine Interaktion über das Internet nicht die gleiche ist wie die Interaktion mit einem Menschen persönlich. Es ist schwer zu sagen, ob jemand lügt, wenn man ihn nicht sehen kann und wenn die E-Mail, die er sendet, genauso aussieht wie eine echte E-Mail von einer Person Ihres Vertrauens. Nichtsdestotrotz gibt es Möglichkeiten, wie Sie die Abwehr Ihres Unternehmens gegenüber dieser Art von Hacking verbessern können. Unternehmen Sie ein paar einfache Schritte:

Wenn sich etwas merkwürdig anfühlt, oder zu gut, um wahr zu sein, dann ist es wahrscheinlich auch so! Wenn Sie z.B. eine Bestätigung über einen Kauf von etwas erhalten, was Sie nie bestellt haben, ist es ratsam, den Absender zu überprüfen.

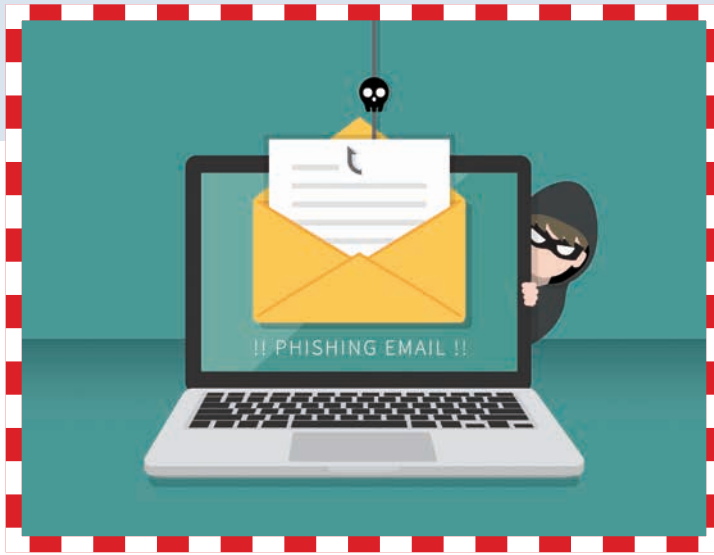
Social Engineering beruht oft darauf, ein Gefühl der Dringlichkeit, Angst oder andere intensive Gefühle zu erzeugen. Unter solchen Umständen ist es leicht, einen Fehler zu machen. Bevor Sie auf einen Link oder E-Mail-Anhang klicken, nehmen Sie sich einen Moment Zeit zum Nachdenken.

Ziehen Sie in Erwägung, Ihre Beschäftigten an einem Schulungsprogramm für Cyber-Sicherheitsbewusstsein teilnehmen zu lassen. In fast allen Fällen verwenden Cyberkriminelle die gleichen Social Engineering-Techniken, um Unternehmen hereinzulegen. Schon die Kenntnis dieser Techniken kann Ihnen helfen, wachsamer zu sein. Es handelt sich um eine Investition, die Ihnen auf lange Sicht viel ersparen kann.

Geben Sie nicht zu viel von sich preis! Beschränken Sie die Informationen, die Sie online veröffentlichen, auf das notwendige Minimum. Social Engineers nutzen routinemäßig Online-Informationen, zum Beispiel aus sozialen Medien, um ihre Botschaften an Sie vertrauenswürdig erscheinen zu lassen. Es ist gut, im Betrieb eine Social-Media-Richtlinie zu entwickeln, die die Privatsphäre aller Beschäftigten berücksichtigt und eine übermäßige Verbreitung persönlicher Informationen verhindert.

Sie sollten eine Zwei-Faktor-Authentifizierung in allen kritischen Systemen Ihres Betriebs, wie z.B. dem Zugriff auf Kundendaten, einführen. Wenn auf diese Weise ein Passwort gehackt wird, kann der Hacker nicht auf alle Ihre Systeme zugreifen.

Machen Sie Ihre Beschäftigten zu „menschlichen Sensoren" und vermitteln Sie ihnen das Gefühl, dass Ihnen das Problem der Cybersicherheit wichtig ist. Wenn sie mit einem Social-Engineering-Versuch konfrontiert werden, sollten sie diese Information unbedingt innerhalb des Unternehmens weitergeben, auch wenn sie nicht darauf hereingefallen sind. Andere im Betrieb könnten das Ziel einer ähnlichen Attacke werden und darauf hereinfallen.

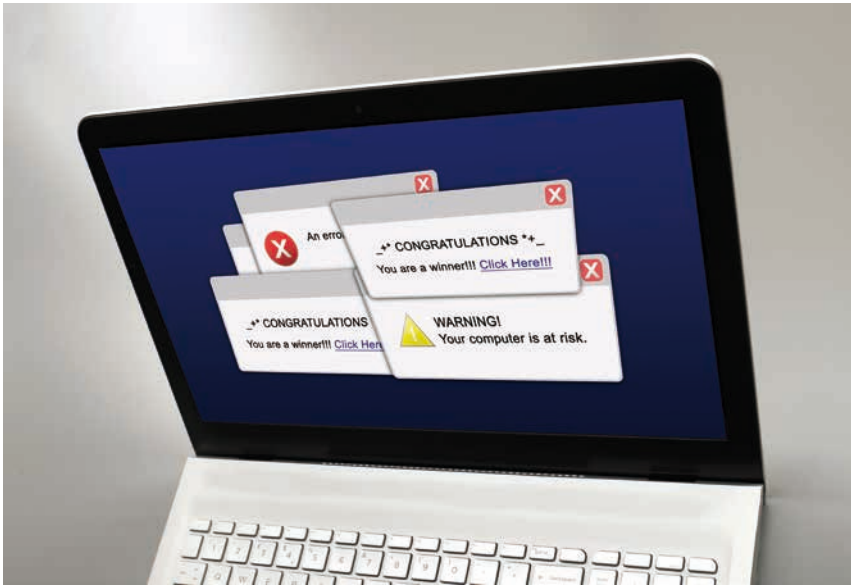


Weitergehende Informationen

1 **Bundesamt für Sicherheit in der Informationstechnik:**
www.bsi.bund.de/DE/

2 **Rat der Europäischen Union:**
https://www.consilium.europa.eu/de/policies/cybersecurity/

3 **Deutschland sicher im Netz:**
https://www.sicher-im-netz.de/social-engineering-und-phishing-erkennen



6 Tipps zum Schutz Ihres Unternehmens gegen Social Engineering

1. Wenn sich etwas zu seltsam anfühlt oder zu gut ist, um wahr zu sein, vertrauen Sie Ihrem Instinkt.

2. Bevor Sie auf einen Link oder E-Mail-Anhang klicken, nehmen Sie sich einen Moment Zeit, um zu überlegen, ob Sie das wirklich tun sollten.

3. Denken Sie darüber nach, in eine Weiterbildung für Ihre Mitarbeitenden zu investieren, die das Bewusstsein für Sicherheit verbessert.

4. Beschränken Sie das, was Sie in sozialen Medien veröffentlichen, auf das Notwendigste.

5. Erwägen Sie, kritischen Systemen eine Zwei-Faktor-Authentifizierung hinzuzufügen.

6. Bitten Sie Ihre Mitarbeitenden, jeden Versuch von Social Engineering zu melden.

issa | INTERNATIONALE VEREINIGUNG FÜR SOZIALE SICHERHEIT | IVSS

Sektion für Maschinen- und Systemsicherheit

IVSS Sektion
Maschinen- und Systemsicherheit

Projektgruppe Digital Manufacturing

Dynamostraße 7–11 · 68165 Mannheim
Deutschland
Telefon: +49 (0) 621 4456 2213
Fax: +49 (0) 3212 1419 443

www.safe-machines-at-work.org

AUVA

BGN
Berufsgenossenschaft
Nahrungsmittel und Gastgewerbe

IFA
Institut für Arbeitsschutz der
Deutschen Gesetzlichen Unfallversicherung

INAIL
ISTITUTO NAZIONALE PER L'ASSICURAZIONE CONTRO GLI INFORTUNI SUL LAVORO

suva

TECHNICAL UNIVERSITY OF KOŠICE

UNIVERSITY of GREENWICH