WHITEPAPER – letzte Überarbeitung März 2024

11 aktuelle Maschen

Die Taktiken der Cyberkriminellen und
wie Sie sich davor schützen können.

GLENDE CONSULTING

Cyberkriminalität stellt eine zunehmend gravierende Gefahr im digitalen Raum dar. In einem Umfeld, das durch rasante technologische Fortschritte geprägt ist, adaptieren auch Cyberkriminelle fortlaufend ihre Methoden, um sowohl Unternehmen als auch Einzelpersonen zu kompromittieren. Dieses Whitepaper beleuchtet 11 gängige Betrugsmuster, die von Cyberkriminellen verwendet werden, und erläutert, wie diese identifiziert und ihnen effektiv begegnet werden kann.

Ziel dieses Whitepapers ist es, ein tiefgreifendes Bewusstsein für diese Bedrohungen zu schaffen und praxisnahe Handlungsanweisungen zu bieten, um Ihre digitale Sicherheit zu stärken.

Support-Masche von einem externen Unternehmen

ABLAUF Stellen Sie sich vor, jemand kontaktiert Sie und gibt sich als Mitarbeiter eines bekannten IT-Support-Unternehmens aus. Diese Person behauptet, es gäbe ein dringendes Problem mit Ihrer IT-Infrastruktur. Sie werden aufgefordert, dem Anrufer Fernzugriff auf Ihren Computer zu gewähren oder vertrauliche Informationen preiszugeben.

ZIEL Das tatsächliche Ziel dieser Betrüger ist es, Zugang zu Ihren Netzwerken zu erhalten oder Schadsoftware zu installieren, um Daten zu stehlen oder Systeme zu kompromittieren.

SCHUTZMASSNAHME Seien Sie wachsam und teilen Sie keine sensiblen Informationen mit, ohne die Identität der Person zu überprüfen. Sprechen Sie solche Anfragen immer mit Ihrem internen IT-Support ab, bevor Sie handeln.

Support-Masche von vermeintlichem internen Support

ABLAUF Wenn Sie Nachrichten erhalten, die angeblich von Ihrem internen IT-Support stammen und sofortige Aktionen, wie das Klicken auf Links oder Öffnen von Anhängen verlangen, seien Sie vorsichtig.

ZIEL Diese Nachrichten zielen darauf ab, Ihre Anmeldeinformationen zu stehlen oder Sie dazu zu verleiten, Malware zu installieren, indem sie sich als legitime Anfragen Ihres IT-Supports ausgeben.

SCHUTZMASSNAHME Informieren Sie sich über die offiziellen Kommunikationskanäle Ihres Unternehmens. Bei Zweifeln überprüfen Sie die Anfrage direkt beim IT-Support.

Falsche Behörden-Masche wegen angeblichen Hacks

ABLAUF Sie erhalten eine Nachricht, die scheinbar von einer Behörde wie dem BSI stammt und die Sie über einen vermeintlichen Hack Ihrer Daten informiert.

ZIEL Die Betrüger versuchen, Sie durch die Vorstellung einer dringenden und ernsten Lage dazu zu bringen, persönliche Informationen preiszugeben oder auf gefährliche Links zu klicken.

SCHUTZMASSNAHME Verifizieren Sie solche Kontaktaufnahmen stets über die offiziellen Kommunikationswege der angeblichen Behörde. Geben Sie keine persönlichen Informationen heraus, bevor Sie die Echtheit der Anfrage bestätigt haben.

Unfall oder Notfall-Masche

ABLAUF Ein Betrüger teilt Ihnen mit, dass eine Ihnen nahestehende Person in einen Notfall verwickelt sei und dringend Ihre Hilfe benötige, oft finanzieller Art oder durch die Weitergabe sensibler Daten.

ZIEL Die Masche spielt mit Ihrer Hilfsbereitschaft und Ihrem Mitgefühl, um Sie in einem schwachen Moment zu einer unüberlegten Handlung zu bewegen.

SCHUTZMASSNAHME Bleiben Sie ruhig und überstürzen Sie nichts. Überprüfen Sie die Situation, indem Sie direkt Kontakt mit der betroffenen Person aufnehmen oder die Informationen über unabhängige Wege verifizieren, bevor Sie handeln.

Fake-Shop-Masche

ABLAUF Sie stoßen beim Online-Shopping auf einen Shop, der hochwertige Produkte zu auffallend niedrigen Preisen anbietet. Nach der Bestellung und Bezahlung stellt sich heraus, dass die Ware nie geliefert wird und der Shop nicht mehr erreichbar ist.

ZIEL Das Ziel dieser Masche ist es, Ihre Zahlungsinformationen zu erlangen und Ihr Geld zu kassieren, ohne die versprochene Ware zu liefern.

SCHUTZMASSNAHME Prüfen Sie die Glaubwürdigkeit des Online-Shops, bevor Sie einen Kauf tätigen. Suchen Sie nach Bewertungen und Erfahrungsberichten und achten Sie auf Gütesiegel und sichere Zahlungsmethoden.

Krisen-Masche (Versprechung einer Förderung/Entschädigung bei Antragstellung)

ABLAUF Sie erhalten eine Nachricht, die behauptet, Sie hätten Anspruch auf finanzielle Unterstützung oder Entschädigung aufgrund einer Krise oder eines Notfalls. Ihnen wird versprochen, dass Sie diese Förderung erhalten können, wenn Sie einen Antrag ausfüllen und persönliche Daten angeben.

ZIEL Die Angreifer versuchen, Ihre persönlichen Daten zu sammeln oder Sie dazu zu bringen, Anmeldeinformationen oder Zahlungsinformationen auf gefälschten Antragsformularen einzugeben.

SCHUTZMASSNAHME Gehen Sie niemals auf solche Angebote ein, ohne sie durch direkte Kontaktaufnahme mit den offiziellen Stellen zu überprüfen. Offizielle Behörden würden niemals sensible Daten über unsichere Kanäle anfordern.

Falsche Webseite-Masche

ABLAUF Sie klicken auf einen Link, der Sie zu einer Webseite führt, die einer offiziellen Seite täuschend ähnlich sieht. Hier werden Sie aufgefordert, sich anzumelden oder persönliche Daten einzugeben.

ZIEL Diese Webseiten sind darauf ausgelegt, Ihre Anmeldeinformationen oder persönlichen Daten zu stehlen.

SCHUTZMASSNAHME Geben Sie niemals persönliche Informationen auf einer Webseite ein, wenn Sie nicht sicher sind, dass es sich um die offizielle Seite handelt. Überprüfen Sie die URL und suchen Sie nach Sicherheitsmerkmalen wie dem HTTPS-Protokoll und dem Schlosssymbol.

PayPal-Freunde-Masche

ABLAUF Sie werden aufgefordert, eine Zahlung über die Option »Geld an Freunde und Familie senden« bei PayPal zu tätigen, oft im Rahmen eines Online-Kaufs, bei dem keine Gebühren anfallen und kein Käuferschutz besteht.

ZIEL Betrüger nutzen diese Methode, um Zahlungen zu erhalten, ohne dass Sie als Käufer Anspruch auf Rückforderung haben, falls die Ware nicht geliefert wird.

SCHUTZMASSNAHME Nutzen Sie beim Online-Kauf immer den offiziellen Zahlungsweg mit Käuferschutz. Seien Sie misstrauisch, wenn Verkäufer speziell auf die Nutzung von »Geld an Freunde und Familie senden« bestehen, besonders bei größeren Beträgen oder bei Anbietern, die Sie nicht persönlich kennen. Überprüfen Sie die Vertrauenswürdigkeit des Verkäufers und bestehen Sie auf einen geschützten Zahlungsdienst, wenn Sie online einkaufen.

Fake-SMS-Masche

ABLAUF Smishing erfolgt über SMS-Nachrichten. Sie erhalten eine SMS, die Sie beispielsweise über ein Problem mit Ihrem Bankkonto informiert und Sie dazu auffordert, auf einen Link zu klicken.

ZIEL Ziel ist es, Sie dazu zu bringen, auf einen Link zu klicken, der Sie zu einer gefälschten Webseite führt, auf der Sie Ihre Daten eingeben sollen.

SCHUTZMASSNAHME Klicken Sie nicht auf Links in SMS-Nachrichten von unbekannten Absendern. Kontaktieren Sie bei Zweifeln die entsprechende Institution direkt über einen bekannten und sicheren Kontaktweg.

Deep Fakes (Nur Audio oder Video und Audio)

ABLAUF Sie erhalten ein Video- oder Audiofile, in dem eine vertraute Person zu sehen oder zu hören ist, die Sie um Hilfe bittet oder Sie zu einer bestimmten Handlung auffordert.

ZIEL Mit Deep Fakes wird versucht, Sie durch die Täuschung, es handle sich um eine echte Nachricht von einer vertrauten Person, zu manipulieren.

SCHUTZMASSNAHME Seien Sie skeptisch gegenüber audiovisuellen Inhalten, die ungewöhnliche Anfragen enthalten. Überprüfen Sie die Echtheit durch direkte Rückfrage bei der betreffenden Person über einen anderen, sicheren Kommunikationskanal.

Live Deep Fake-Masche

ABLAUF In einer Videokonferenz erscheint plötzlich ein Kollege, Vorgesetzter oder Geschäftspartner, der unerwartet um vertrauliche Informationen bittet oder Sie zu sofortigen finanziellen Transaktionen auffordert.

ZIEL Hierbei wird Deep Fake-Technologie in Echtzeit eingesetzt, um Sie glauben zu machen, dass Sie mit einer echten Person sprechen. Das Ziel ist es, sensible Informationen zu erbeuten oder Sie zu finanziellen Handlungen zu verleiten.

SCHUTZMASSNAHME Seien Sie besonders vorsichtig bei Anfragen über Videokonferenzen. Wenn Sie Zweifel an der Identität der Person haben, unterbrechen Sie das Gespräch und überprüfen Sie die Anfrage über bekannte und verifizierte Kontaktdaten. Vertrauen Sie auf etablierte Sicherheitsprotokolle, insbesondere wenn es um vertrauliche oder finanzielle Anfragen geht.

DIE WARNSIGNALE, BEI DENEN SIE MISSTRAUISCH WERDEN SOLLTEN, SIND IMMER IDENTISCH.

Erschaffung eines falschen Gefühls der Dringlichkeit
Betrüger stellen häufig dringende Anforderungen, wie beispielsweise den sofortigen Handlungsbedarf zur Vermeidung des Verlusts von Daten, um eine schnelle Reaktion ohne gründliche Prüfung zu provozieren.

Verwendung von Drohungen
Einschüchterungen, wie bspw. die Androhung der Kontosperrung bei Nichtbereitstellung von Daten, sind ein gängiges Instrument, um Druck aufzubauen.

Aufforderungen zur Preisgabe sensibler Informationen
Cyberkriminelle fordern oft vertrauliche Details wie PINs oder Kreditkartennummern unter dem Vorwand offizieller Notwendigkeiten.

Präsenz von Links und Formularen in Kommunikationen
E-Mails, die Links oder Formulare enthalten, können mit Malware infiziert sein, die zur Extraktion sensibler persönlicher Informationen dient.

Verdächtige Nachrichten von bekannten Absendern
Korrespondenz, die angeblich von vertrauten Personen oder Organisationen stammt, aber ungewöhnliche Merkmale wie einen seltsamen Betreff oder unpassenden Zeitpunkt aufweist, kann ein Indiz für Phishing sein.

Um sich vor Cyberkriminalität zu schützen, ist es essenziell, niemals auf unverlangte Aufforderungen zur Angabe sensibler Informationen zu reagieren. Kein legitimes Kreditkartenunternehmen und kein seriöser Dienstleister wird solche Daten per E-Mail anfordern.

ZUSÄTZLICHE SICHERHEITSMASSNAHMEN ERGREIFEN

Verifizierung der Adresszeile im Browser
Durch das Setzen von Lesezeichen für häufig besuchte Seiten können Sie vermeiden, auf gefälschte Websites zu gelangen.

Vorsicht bei verdächtigen Links in E-Mails
Anstatt auf Links zu klicken, sollten Sie die betreffende Webseite direkt über die Startseite der Organisation aufrufen. Die »Mouse-over« (bewegen Sie den Mauszeiger über den Link, ohne ihn anzuklicken) Technik kann ebenfalls helfen, die wahre URL hinter einem Link zu identifizieren.

Verifizierung bei Unsicherheit
Wenn Zweifel an der Legitimität einer E-Mail bestehen, kontaktieren Sie die Organisation direkt telefonisch.

Keine Weitergabe persönlicher Daten per E-Mail
Übermitteln Sie niemals persönliche Identifikatoren wie PINs oder Passwörter elektronisch.

Aufmerksamkeit bei Online-Transaktionen
Falls bei der Dateneingabe auf vertrauten Websites Unstimmigkeiten auffallen, beenden Sie die Sitzung umgehend und kontaktieren Sie den Anbieter.

Vermeidung von Downloads aus E-Mails
Verwenden Sie ausschließlich offizielle Download-Links von der Webseite des Anbieters.

Kein Öffnen von Anhängen in verdächtigen E-Mails
Anhänge können Malware enthalten und sollten nicht geöffnet werden.

Reguläres »Logout« bei Online-Sitzungen
Schließen Sie nicht einfach das Browserfenster, sondern führen Sie stets einen ordnungsgemäßen Logout durch.

Kontinuierliche Kontrolle der Kontoauszüge
Bei Unregelmäßigkeiten sollten Sie schnellstmöglich reagieren.

Achten auf verschlüsselte Verbindungen
Eine sichere Webseite erkennen Sie am »https://« und einem Schloss-Symbol in der Adresszeile.

Entscheiden Sie sich für uns, ist es plötzlich ganz einfach.

WIR KÜMMERN UNS UM DATENSCHUTZ UND INFORMATIONSSICHERHEIT IN IHREM UNTERNEHMEN:

SO KONFORM WIE NÖTIG - SO PROZESSORIENTIERT WIE MÖGLICH!

glende-consulting.de

» BESUCHEN SIE UNS

GLENDE.CONSULTING GmbH & Co. KG
Friedrich-Barnewitz-Str. 7
18119 Rostock-Warnemünde

» SPRECHEN SIE MIT UNS

Tel.: 0381.7787 468-0

» SCHREIBEN SIE UNS

info@glende-consulting.de