DSD28

Willkommen zum Datenschutz-Webinar 03-2022

Inhalt

DSD28

1. Schwerpunktthema: Social Engineering
   Der Mensch als größtes Sicherheitsrisiko im Betrieb
2. Neues aus den Aufsichtsbehörden und Gerichten

Social Engineering

DSD28

Was ist Social Engineering?

- Beim Social Engineering werden menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Cyber-Kriminelle verleiten das Opfer auf diese Weise beispielsweise dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.
- Social Engineering ist an sich nichts Neues und dient seit Menschengedenken als Grundlage für die unterschiedlichsten Betrugsmaschen. Im Zeitalter der digitalen Kommunikation ergeben sich jedoch äußerst effektive, neue Möglichkeiten für Kriminelle, mit denen sie Millionen von potenziellen Opfern erreichen können.

Quelle: BSI https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html

Social Engineering

DSD28

Das Ziel:

Ein Opfer, das auf die Täuschung hereinfällt, handelt im guten Glauben, das Richtige zu tun.

Quelle: BSI https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Social-Engineering/social-engineering_node.html

Wer ist Ziel solcher Angriffe?

Social Engineering ist mittlerweile eine der größten Formen von Sicherheitsbedrohungen für alle Arten von Unternehmen geworden, bei welcher gezielt die Menschlichkeit ausgenutzt wird.

Social Engineering - Arten

DSD28

Pretexting – Schaffen eines Vorwands

Bei dieser Form von Social Engineering konzentrieren sich die Angreifer darauf, einen **guten Vorwand** bzw. **ein erfundenes Szenario** zu schaffen, das sie nutzen können, um Zugang zu sensiblen Daten oder geschützten Systemen zu erlangen. Dieses Szenario besteht aus glaubwürdigen aber erfundenen Geschichten zur persönlichen oder geschäftlichen Verbindung zum Unternehmen. Beispielsweise gibt sich ein Angreifer als Mitarbeiter der IT-Abteilung aus, um sein Opfer z.B. dazu zu verleiten, Login-Daten preiszugeben.

Social Engineering - Arten

DSD28

Tailgating – der Angreifer direkt vor der Tür

Bei Tailgating liegt der Fokus des Angreifers darauf, **physischen Zugang zu einem Firmengelände** zu erhalten. Ein Beispiel für eine wäre, wenn sich der Angreifer als Fahrer einer Lieferfirma ausgibt und darauf wartet, Zutritt zum Firmengelände zu erhalten, durch jemanden, der autorisiert ist. Auch können Angreifer vortäuschen, z.B. die Zugangskarte zum Gebäude vergessen zu haben.

Social Engineering - Arten

DSD28

Phishing-Angriffe – das betrügerische Angeln von sensiblen Daten

Beim Phishing geben sich die Angreifer als **vertrauenswürdige Quelle** aus und nehmen betrügerische Kommunikation mit ihrem Opfer auf. Häufig wird dazu in einer **E-Mail** ein **Link** verschickt, welcher scheinbar auf eine vertraute Webseite verweist. In Wirklichkeit führt dieser Link aber auf eine täuschend echte Webseite. Gibt der Nutzer dort z.B. seine Benutzerdaten ein, so „fischt“ der Angreifer die Daten ab.

Social Engineering - Arten

DSD28

Spear-Phishing – das gezielte Angeln

Das Spear-Phishing ist eine Sonderform des Phishings und zielt auf einen **individuellen Angriff** eines **spezifischen Unternehmens** oder einer **bestimmten Person** ab. Die Empfänger werden hierbei sorgfältig ausgewählt und erhalten z.B. E-Mails, die persönlich auf sie zugeschnitten sind, um so Vertrauen zu gewinnen.

Social Engineering - Arten

DSD28

CEO-Fraud – der Chef-Trick

Die Angreifer geben sich z.B. in einer gefälschten E-Mail oder in einem Telefonat als Geschäftsführer oder Vorstandsmitglied aus und fordern sofortige Mitteilung vertraulicher Daten. Hier wird besonders auf das typische Merkmal von Social Engineering gesetzt – „**unter Druck setzen**“. Diese Art von Angriff kann sehr schnell gelingen, da man zunächst keine Zweifel hegt – denn es ist ja der eigene Chef. Die Angreifer erkunden dabei schon lange im Vorfeld das Unternehmen und den Vorgesetzten aus, um täuschend echt zu wirken.

Social Engineering - Arten

DSD28

Baiting – der Köderangriff

Beim Baiting wird auf die **Neugier** oder **Gier** des Opfers gesetzt. Angreifer verwenden physische oder digitale Gegenstände, hinter denen sich zumeist Malware verbirgt. Solche Gegenstände sind beispielsweise Download-Links, die ein kostenloses Programm oder einen kostenlosen Musikdownload versprechen. Ein beliebter Köder ist z.B. auch ein **USB-Stick** mit scheinbar interessanten Daten.

Social Engineering - Arten

DSD28

Quid pro quo – ein Geben und Nehmen

Quid pro quo-Angriffe versprechen einen **Vorteil gegen Informationen oder Handlung**. Ein typisches Szenario im Unternehmen wäre die Imitierung eines Angreifers als ein IT-Servicemitarbeiter, der seine IT-Unterstützung anbietet und eine schnelle Lösung verspricht, wenn der Mitarbeiter z.B. das Antivirenprogramm deaktiviert, weil er davon ausgeht, es handle sich um ein Software-Update.

SE - Gegenmaßnahmen

DSD28

Keine vertraulichen Gespräche an öffentlichen Orten

Wer regelmäßig mit öffentlichen Verkehrsmitteln unterwegs ist, kennt sie zur Genüge, die **Vieltelefonierer**. Mit lauter Stimme führen sie Gespräche, die ihr unmittelbares Umfeld wenig bis gar nicht interessieren. Dass sie dabei den Umstehenden auch – mitunter erstaunlich sensible – Informationen über ihr Unternehmen preisgeben, ist ihnen nicht bewusst.

SE - Gegenmaßnahmen

DSD28

Vorsicht in sozialen Netzwerken

Oftmals spähen Täter ihre Opfer vor der Attacke aus. Je mehr eine Person über sich im Internet preisgibt, desto gefährdeter ist sie. Auch hier ist der Schutz denkbar einfach: Informationen, die den Arbeitgeber betreffen, sollten Mitarbeiter nur in Absprache mit der Geschäftsleitung im Internet veröffentlichen. Bei der Veröffentlichung von privaten Informationen sollte der Nutzer die Privatsphäre-Einstellungen der Social-Media-Portale nutzen und nur ihm tatsächlich bekannten Personen den Zugriff auf persönliche Informationen erlauben.

SE - Gegenmaßnahmen

DSD28

Vorsicht bei E-Mails und Dateianhängen

Links in E-Mails mit kryptischen Betreffzeilen, die vielleicht zudem von unbekannten Personen stammen, sollten Mitarbeiter nicht öffnen. Gleiches gilt für Dateianhänge, deren Ursprung nicht genau ersichtlich ist. Nicht selten enthalten solche verlinkten Webseiten und Dateianhänge Schadsoftware, die z.B. Fremden den Zugriff auf unternehmensinterne Ressourcen ermöglichen.

SE - Gegenmaßnahmen

DSD28

Gesundes Misstrauen gegenüber Fremden

Gerade in Großunternehmen, in denen nicht mehr jeder Mitarbeiter jeden Kollegen persönlich kennt, kommt es vor, dass sich Betriebsfremde als neue Mitarbeiter oder Dienstleister ausgeben und auf diese Weise im Unternehmen Informationen ausspähen. Hier gilt: Gegenüber fremden Personen sollte man ein gesundes Misstrauen pflegen. Bevor man an sie vertrauliche Informationen herausgibt, sollte man die Identität der Person prüfen.

SE - Gegenmaßnahmen

DSD28

Lieber einmal zu viel nachfragen als zu wenig

Die Überschrift sagt schon alles!

News

DSD28

Aus den Gerichten und Aufsichtsbehörden

1. 1,9 Mio-€ für BREBAU
2. OLG dresden: Geschäftsführer ist Verantwortlicher

BREBAU

DSD28

03.03.2022:

„Am heutigen Tage hat die Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) als datenschutzrechtliche Aufsichtsbehörde die BREBAU GmbH mit einer Geldbuße nach Artikel 83 Datenschutzgrundverordnung (DSGVO) belegt. “

BREBAU

DSD28

„Die BREBAU GmbH hat mehr als 9.500 Daten über Mietinteressent:innen verarbeitet, **ohne** dass es hierfür eine **Rechtsgrundlage** gab.

Beispielsweise Informationen über **Haarfrisuren**, den **Körpergeruch** und das **persönliche Auftreten** sind für den Abschluss von Mietverhältnissen nicht erforderlich. Bei mehr als der Hälfte der Fälle handelte es sich darüber hinaus um Daten, die nach der DSGVO besonders geschützt sind. Rechtswidrig verarbeitet wurden auch Informationen über die **Hautfarbe**, die **ethnische Herkunft**, die **Religionszugehörigkeit**, die **sexuelle Orientierung** und über den **Gesundheitszustand**. Auch hat die BREBAU GmbH Anträge Betroffener auf Transparenz über die Verarbeitung ihrer Daten bewusst konterkariert. “

BREBAU

DSD28

„Die nach Artikel 83 DSGVO verhängte Geldbuße beläuft sich auf rund 1,9 Millionen Euro. Der außerordentlichen Tiefe der Verletzung des Grundrechts auf Datenschutz wäre eine **deutlich höhere Geldbuße angemessen gewesen**. Weil die BREBAU GmbH im datenschutzrechtlichen Aufsichtsverfahren **umfassend kooperierte**, sich um **Schadensminderung**, **eigene Aufklärung des Sachverhalts** und darum bemühte, dass **entsprechende Verstöße sich nicht wiederholen**, konnte die Höhe der Geldbuße erheblich reduziert werden “

Geschäftsführer

DSD28

„OLG Dresden: Geschäftsführer haften persönlich für Datenschutzverstöße der GmbH“

Das Oberlandesgericht Dresden (Urt. v. 30.11.2021 – 4 U 1158/21) hat eine Gesellschaft und ihren Geschäftsführer als Gesamtschuldner zur Zahlung von 5.000 Euro DSGVO-Schadensersatz verurteilt. Das Gericht ging dabei davon aus, dass neben der Gesellschaft auch der Geschäftsführer als eigener datenschutzrechtlich Verantwortlicher einzustufen sei und daher für den Datenschutzverstoß persönlich hafte.

Geschäftsführer

DSD28

Ausblick in die Zukunft:

Sollten sich weitere Gerichte der Auffassung der Dresdner Richter anschließen, hätte dies weitreichende Folgen für die Praxis. Geschäftsführer müssten dann damit rechnen, wegen Datenschutzverstößen persönlich in Haftung genommen zu werden. Dieses Haftungsrisiko besteht insbesondere dann, wenn sie die dem Datenschutzverstoß zugrundeliegende Datenverarbeitung selbst initiiert haben oder an entsprechenden Entscheidungen oder Beauftragungen mitgewirkt.

DSD28

Vielen Dank