Von Antivirus bis Zero-day-Exploit:

20 Begriffe zur Cybersicherheit, die du kennen solltest

NordVPN®

“

Cybersicherheit betrifft all unsere Online-Aktivitäten.Mehr als je zuvor verschmelzen das Online-Leben und das „normale“ Leben miteinander. Infolgedessen sind Bedrohungen der Cybersicherheit gleichzeitig Bedrohungen unserer Lebensgrundlagen, und Aufklärung stellt die Grundlage für den Schutz unseres Wohlbefindens dar. Jeder profitiert von Grundkenntnissen. Daher sollten alle das A-Z der Cybersicherheitsbegriffe beherrschen.

Troy Hunt

Troy Hunt - Mitglied des Beratungsgremiums bei NordVPN, Regionaldirektor bei Microsoft und Most Valuable Professional for Developer Security, Blogger auf troyhunt.com, internationaler Redner zum Thema Websicherheit, sowie Autor vieler hochgelobter Sicherheitskurse für Webentwickler auf Pluralsight.

Vorwort

Wenn du dich im Bereich Cybersicherheit orientieren möchtest geben wir die einen Wegweiser an die Hand.. Denn das, was üblicherweise passiert, wenn du nach Informationen zum Schutz im Netz suchst, ist Folgendes: Du stolperst über das Wort Spyware und möchtest wissen, was es bedeutet.

In dem Moment, indem du nachzuschauen beginnst, überwältigen dich Begriffe, die du nie zuvor gehört hast. Nehmen wir als Beispiel eine kurze Definition.

> Spyware ist eine Art der Malware, die das Gerät des Opfers überwacht, um ohne das Wissen des Opfers sensible Daten abzugreifen. Beispiele von Spyware sind: Adware, Keylogger und Trojaner.

Die Definition ist richtig, aber sie ist nicht wirklich hilfreich. Jetzt hast du mehr Fragen. Wie funktioniert Spyware? Was sind sensible Daten, und wie besorgt solltest du über ihre Sicherheit sein? Was ist ein Keylogger? Ist das überhaupt ein Wort?

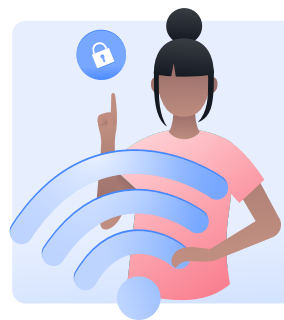
Wir verfolgen einen anderen Ansatz

Statt technische Erklärungen zu liefern, zeigen wir, wie Cybersicherheit unser Leben beeinflusstund liefern praxisnahe Vergleiche. Es handelt sich nicht um ein umfangreiches Glossar. Und so ist es auch beabsichtigt. Es soll Lust auf eine Vertiefung der Themen machen.

Wenn du nach detaillierteren, technischeren Erklärungen zu allen Dingen der Online-Sicherheit suchst, besuche unseren Blog auf NordVPN.com/-blog, wo du sowohl beliebte als auch tiefergehende Informationenfindest.

Inhaltsverzeichnis:

3 Antivirus
4 Botnetz
5 Geheimtext
6 Datenschutzverletzung
7 End-to-End-Verschlüsselung
8 Firewall
9 Hacker
11 IP addresse
12 Cryptojacking
13 Keylogger
14 Logikbombe
15 Man-in-the-Middle-Angriff
16 Netzwerk
17 Phishing
18 Ransomware
19 Social Engineering
21 Zwei-Faktor-Authentifizierung
22 VPN
23 WLAN
24 Zero-day-exploit



A

Antivirus

Du hast eine neue E-Mail bekommen. Betreff: **Ich liebe dich**

Darin findest du eine wunderschöne Liebeserklärung eines anonymen Bewunderers. Und es gibt auch ein Foto. Neugierig klickst du auf den Anhang - und lädst ein Virus herunter.

Dein Antiviren-Programm stellt ihn umgehend unter Quarantäne. Du hast Glück gehabt - es ist ein alter Virus, seine Signatur befindet sich bereits in der Datenbank.

Wenn der Virus neu und nicht in der Datenbank registriert ist, kann das Antiviren-Programm andere Tools verwenden, um ihn zu entdecken. Es überprüft deinen Computer auf verdächtige Aktivitäten. Sollte ein Programm versuchen, das Antiviren-Programm zu umgehen, es beim Start ohne Erlaubnis laufen oder andere Schadsoftware herunterladen, reagiert das Antiviren-Programm.

Und es sind nicht nur Viren. Es gibt alle möglichen Arten von schädlicher Software - Trojaner, Ransomware, Keylogger, etc. - die versuchen, deine Geräte zu gefährden oder zu missbrauchen.

Heutzutage steht das Wort „Antivirus“ für alle möglichen Anti-Schadsoftware-Tools, die Geräte vor Schadsoftware schützen.

Verwandte Begriffe: Virus, Schadsoftware, Anti-Schadsoftware, Trojaner, Wurm, Adware.

B

Botnetz

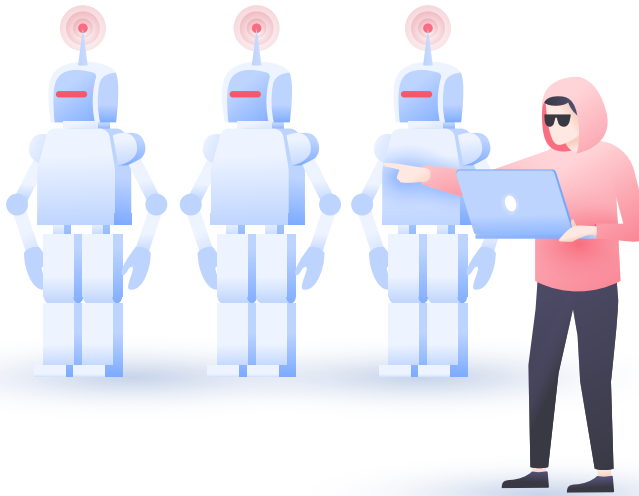
Du öffnest deinen Browser, gibst die Adresse deiner Lieblings-Meme-Webseite ein. Oh, sie ist nicht verfügbar. Und du wirst niemals erraten, wieso.

Es sind Zombies.

Bots, um genau zu sein. Ein Schwarm an gedankenlosen, infizierten Geräten hat hunderttausende Anfragen an die Webseite gesendet und sie zum Absturz gebracht.

Diese Attacke wird DDoS genannt, was für Distributed Denial of Service steht. Leute nutzen Botnetze für solche und andere schändliche Zwecke, wie E-Mail-Spam oder künstlich geschaffenen Internet-Traffic.

Deine Geräte können auch Teil eines Botnetzes sein, die heimlich den Befehlen eines Cyberkriminellen gehorchen. Es ist schwer zu wissen, ob dein Computer ein Bot ist - die einzigen Anzeichen können eine etwas langsamere Leistung oder eine Überhitzung sein.



Verwandte Begriffe: bot, zombie, DDoS attack.

C

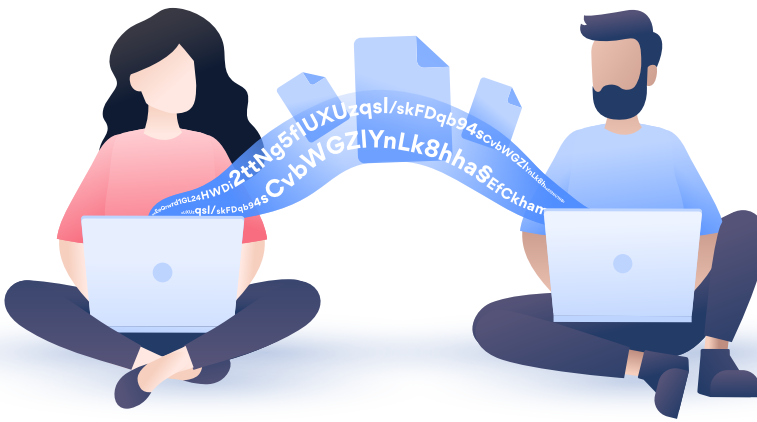
Geheimtext

Du öffnest eine Messaging-App und schreibst, „SORRY, LEUTE, ich schaffe es heute Abend nicht. Ich habe mir wahrscheinlich einen Magen-Darm-Infekt eingefangen.“

Das nennt man Klartext. Es handelt sich um einen unverschlüsselten Text, den jeder Online-Spion abfangen und lesen kann.
Das nennt man auch eine Lüge - du fühlst dich gut, aber du würdest lieber einen Film schauen. Aber immerhin benutzt du eine sichere Messaging-App. Sie wendet einen Algorithmus an, der deine Lüge in einen Geheimtext umwandelt.

> “ueEeQrwrd1GL24HWDi2ttNg5fIUXUzqsIFqb94^Ef2NU1NBrD
> rPb84wbReVnclTP2AgnMCkhaHC3UrfR8VWxh3jWWh+0WE”

Das ist Verschlüsselung in Aktion. Ein Klartext wird mithilfe eines Sicherheitsschlüssels (einer Chiffre) in einen Geheimtext umgewandelt. Die Messaging-Apps, die deine Freunde verwenden, besitzen den Schlüssel, der deine Nachrichten entschlüsselt. Online-Spione haben den Schlüssel nicht und können deine Unterhaltungen nicht lesen.



Verwandte Begriffe: Verschlüsselung, Chiffre, Klartext, entschlüsseln

D

Datenschutzverletzung

Du machst einen Gruppenchat mit einem Haufen deiner engsten Freunde. Eines Tages bemerkst du, dass Screenshots des Chats in den sozialen Medien zirkulieren.

Du hast gerade eine Datenschutzverletzung erlebt. Eine Datenschutzverletzung ist dann der Fall, wenn sensible Daten in die Hände eines Unbefugten fallen.

Wie konnte das passieren? Ein Hacker hat deine Unterhaltungen abgefangen? Oder war es ein Chat-Teilnehmer? Vielleicht ist Marks Mitbewohner dem Chat beigetreten, als Mark nicht am Laptop war. Der sah immer schon zwielichtig aus. Du wirst es wahrscheinlich nie herausfinden.

Das passiert auch bei großen Datenschutzverletzungen in Unternehmen.

Unternehmen sammeln riesige Mengen an Daten - manchmal Daten von Nutzern wie dir - und manche von diesen Unternehmen werden gehackt. Daten sickern durch, und du siehst, wie deine Login-Daten und Passwörter im Web herumschwirren.

Überprüfe regelmäßig, ob deine Konten Opfer einer Datenschutzverletzung geworden sind auf: haveibeenpwned.com.

Verwandte Begriffe: Ungewollte Weitergabe von Informationen, Datenleck, Datenpanne

E

End-to-End-Verschlüsselung

Du hast vielleicht schon einmal eine Nachricht, wie diese gehört: : „Wir führen eine End-to-End-Verschlüsselung ein!“ Was ist daran so „End-to-End“?
Eine End-to-End-Verschlüsselung überspringt den Mittelsmann. Nur du und die Person, der du die Nachricht schickst, können deren Inhalt sehen.

Stell dir deine Daten als Nachricht auf Papier vor. Bevor du sie abschickst, steckst du sie in einen Umschlag, der den Inhalt vor neugierigen Blicken schützt. Das ist Verschlüsselung.

Irgendwann auf dem Weg öffnet ein Dritter (zum Beispiel ein Sofortnachrichtendienst, den du nutzt), diesen Umschlag, entnimmt deine Daten und sendet sie an den Zielort. Auf diese Weise funktioniert das Internet - es gibt überall Mittelsmänner.

Eine End-to-End-Verschlüsselung überspringt den Mittelsmann. Nur du und die Person, der du die Nachricht schickst, können deren Inhalt sehen.

Verwandte Begriffe: Geheimtext, Klartext

F

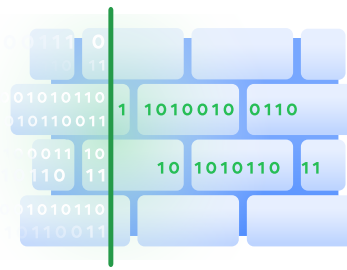
Firewall

Du stehst in einer Schlange. Als du den Türsteher erreichst, sagt dieser: „Kein Zutritt“. Du drehst dich um und gehst nach Hause - kein Club-Abend heute.

Der Türsteher setzt die Regeln durch, wer in den Club darf und wer nicht. Diese Regeln sind willkürlich - sie hängen von den Richtlinien des Clubs und externen Umständen ab. Sie können sich ändern, wenn der Club voll wird oder eine private Party stattfindet.

In gleicher Weise steht eine Firewall zwischen deinem lokalen Netzwerk und dem Internet. Wie ein digitaler Türsteher setzt er die Regeln durch, welcher Traffic gut genug ist, um dein Netzwerk betreten zu dürfen.

Eine Firewall erlaubt Traffic von vertrauensvollen Quellen oder IP-Adressen. Nicht auf der Liste? Tut mir leid, Traffic, dreh um und geh nach Hause. So schützt eine Firewall dein Netzwerk vor böswilligem Internet-Traffic, der dein System gefährden könnte.



H

Hacker

Du kennst sie aus den Filmen. Mysteriös, gefährlich, sogar gesellschaftsfeindlich. Sie sind digitale Outlaws, die unter dem Radar leben. Sie hacken das Pentagon in weniger als fünf Minuten.

Das ist ohne Frage Fiktion. Hacker sind Menschen - und jeder Mensch hat seine Motive. Manche genießen die intellektuelle Herausforderung, in Netzwerke einzudringen. Andere, die sogenannten Black-Hat-Hacker, handeln böswillig. Sie kompromittieren Systeme zum eigenen Vorteil, stehlen wertvolle Daten oder Geld, stören Netzwerke und können alle möglichen Schäden anrichten.

Manche Unternehmen und Regierungen stellen White-Hat-Hacker an, die die Sicherheit der Computersysteme überprüfen, indem sie in sie eindringen. Das nennt man Penetrationstest, der viele Formen haben kann - sogar physische.

Zum Beispiel kann ein White-Hat-Hacker das Unternehmensgebäude betreten, indem er einem Angestellten folgt. Menschen sind höflich - sie halten für gewöhnlich anderen die Türen auf, selbst Fremden. Sobald er ins Innere gelangt ist, kann der Hacker Festplatten mit sensiblen Daten stehlen, auf unbewachte Computer zugreifen oder sie kompromittieren (mit Keyloggern zum Beispiel).

Kannst du gehackt werden?

Das hängt von deinen Sicherheitsmaßnahmen ab. Dennoch können äußerst talentierte Hacker oft einen Weg in das sicherste Netzwerk finden. Die gute Nachricht lautet, dass sie wahrscheinlich lukrativere Ziele im Kopf haben als dein Stream-Konto.

In der Regel leidest du indirekt unter Hackern, siehe: Datenschutzverletzung.

Du solltest dich vor Betrügern in Acht nehmen, die gefälschte Webseiten erstellen und schädliche Links versenden, siehe Phishing. Gib dein Passwort auf einer betrügerischen Webseite ein - und du übermittelst es direkt dem Betrüger.

Verwandte Begriffe: Grey-Hat-Hacker, Black-Hat-Hacker, White-Hat-Hacker, Penetration, Penetrationstests.

I

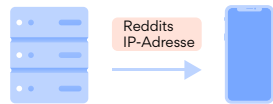
IP-Adresse

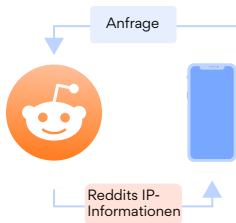
Dein Smartphone besitzt eine IP-Adresse (kurz für Internet-protokoll-Adresse), die von deinem Netzwerk zugewiesen wurde; genauso wie dein Laptop, Smart-TV und andere Geräte, die sich mit dem Internet verbinden. Kein Gerät könnte online ohne eine solche Adresse funktionieren. Wieso?

Sagen wir, du musst etwas Zeit totschlagen. Du nimmst dein Smartphone heraus und tippst „Reddit.com“ in die Adresszeile ein.

Aber dein Smartphone weiß nicht, was „Reddit.com“ bedeutet. Zahlen, nicht Wörter, sind seine Muttersprache. Um auf Reddit zuzugreifen, sendet dein Smartphone eine Frage aus: „Was ist die IP-Adresse von Reddit.com?“

Die Frage geht an einen speziellen Server - eine Datenbank von IP-Adressen. Der Server findet die IP-Adresse von Reddit und sendet sie zurück an dein Smartphone.





Dein Smartphone sendet dann die Anfrage an Reddits IP-Adresse. Reddit sendet die Informationen zurück an die IP-Adresse deines Smartphones.

Eine Sekunde vergeht. Reddit lädt auf deinem Bildschirm. Langweilig, nichts weckt dein Interesse, du verlässt die Seite.

J

Cryptojacking

Dein Computer ist heiß und brummt, der Ventilator dreht sich wie verrückt. Und er ist langsam - du musst eine Weile warten, bevor irgendetwas lädt.

Der Grund? Ein Hacker hat deinen Computer gekapert, um Kryptowährung zu schürfen.

Du hast wahrscheinlich von Cryptomining gehört. Um es einfach auszudrücken: Du erhältst Kryptowährung als Belohnung für die Ausführung komplexer Berechnungen auf deinem Computer. Aber diese Berechnungen verbrauchen sehr viel Computer-Leistung - in der Regel zu viel Leistung, als dass Cryptomining sich lohnen würde.

Um das Problem zu lösen, kapern Hacker Geräte, um für sich selbst Kryptowährung zu schürfen. Sie führen diese Attacken - die man Cryptojacking nennt - durch, indem sie Schadsoftware oder schädliche Codes auf Webseiten verwenden. Ahnungslose Opfer sind verwundert, wieso ihr Computer vorÜberhitzung rot glüht.

P.S.: Ja, wir wissen, dass CryptoJacking eigentlich nicht unter J gehört. Aber was Begriffe zur Cybersicherheit angeht, ist der Buchstabe J eine einsame Wüste, also sind wir kreativ geworden.

Verwandte Begriffe: Cryptomining, schädliches Cryptomining

Keylogger

Du befindest dich in der Bibliothek und schreibst eine Arbeit für deinen Wirtschaftskurs. Sie ist seit gestern überfällig. Die Batterien deines Laptops sind schwach, du hast das Kabel zu Hause vergessen.

Neben dir sitzt eine freundlich aussehende junge Frau. Du fragst nach ihrem Laptop - du brauchst fünf Minuten, um den Gedanken aufzuschreiben, während er noch in deinem Kopf herumschwirrt. Sie hilft dir gerne. Du nimmst ihren Laptop, loggst dich in die Cloud ein und beendest die Kritik an der Kartellpolitik der Depressionszeit.

Als du wieder zu Hause bist, stellst du fest, dass dein E-Mail-Account und viele deiner anderen Online-Accounts gehackt wurden. Wie?

Die Frau hatte einen Keylogger auf ihrem Laptop installiert. Das ist ein Tool, das Tastenanschläge registriert. Es hat alles gespeichert, was du eingegeben hast, einschließlich deines Passworts und des Logins für die Cloud.

Da du dasselbe Passwort für die Cloud und dein E-Mail-Konto verwendest, hat die Hackerin Zugang zu deinem bevorzugten E-Mail-Konto erhalten (aus diesem Grund solltest du Passwörter nur einmal verwenden). Dadurch hat sie die Passwörter deiner anderen Konten zurückgesetzt.

Keylogger kommen selten von freundlich aussehenden jungen Frauen. Normalerweise nehmen sie die Form von Hardware-Geräten an, die Hacker an unbewachten Computern anbringen. Es können auch Software-Tools sein, die sowohl illegal als auch legal verwendet werden. Zum Beispiel installieren manche Unternehmen Keylogger in ihren Computern, um die Angestellten zu überwachen.

Related terms: spyware.

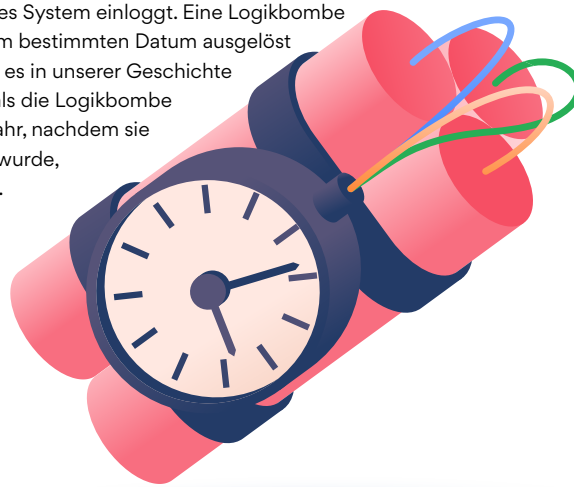
L

Logikbombe

Du bist bei der Arbeit, die Deadline war vor fünf Minuten. Du tippst wütend, als alles abstürzt. Du hast keinen Zugriff auf das interne Netzwerk oder irgendwelche entfernten Dateien. Heute keine Arbeit mehr.

Am nächsten Tag hörst du Gerüchte. Es soll ein ehemaliger Angestellter gewesen sein, ein verärgerter IT-Typ - er hat das interne Netzwerk stillgelegt. Aber wie kann das sein? Er wurde vor einem halben Jahr gefeuert und hatte keinen Zugriff mehr auf die Systeme des Unternehmens.

Na ja, am letzten Tag auf der Arbeit hat er eine Logikbombe hinterlassen. Das ist ein Teil eines schädlichen Codes, der aktiviert wird, wenn bestimmte Bedingungen eintreffen. Wenn sich zum Beispiel der CEO in ein sensibles System einloggt. Eine Logikbombe kann an einem bestimmten Datum ausgelöst werden - wie es in unserer Geschichte passiert ist, als die Logikbombe ein halbes Jahr, nachdem sie eingerichtet wurde, explodiert ist.



Verwandte Begriffe: Zeitbombe, interne Bedrohung

Man-in-the-Middle-Angriff

Du bist in einem Café, verbunden mit dem öffentlichen WLAN-Netz. Du hast gerade eine E-Mail an deinen Auftragnehmer geschickt, indem du nach dessen Kontonummer fragst. Du bekommst die Nummer, bezahlst die Gebühr, trinkst den Cappuccino.

Zwei Tage später meldet sich der Auftragnehmer mit einer Frage: „Wann werde ich bezahlt?“

Was?

Rückblende zum Café. Vor dir kam ein Hacker im Café an, richtete einen Evil-Twin-Hotspot (Böser-Zwilling-Hotspot) ein und nannte ihn „Café KOSTENLOSES WLAN“. In dem Glauben, dass es sich um ein seriöses Netzwerk handelte, hast du dich damit verbunden. Von dem Moment an konnte der Hacker deinen Internetverkehr überwachen.

Das ist ein Man-in-the-Middle-Angriff in Aktion.

Der Hacker hat deine E-Mail abgefangen und dir seine eigene Kontonummer geschickt. Er wurde bezahlt, während dein Auftragnehmer weiter auf seine Gebühr wartet.

Du darfst nicht vergessen, dass ein öffentliches WLAN-Netzwerk kein sicheres Netzwerk ist. Selbst wenn es nicht von einem Hacker eingerichtet wurde, weißt du nie, wie gut es konfguriert ist. Mitten in den Kommunikationen kann jemand lauern. Stelle sicher, dass du ein VPN verwendest, bevor du dich damit verbindest.

Verwandte Begriffe: Evil-Twin-Angriff, Wi-Fi-Honeypot

N

Netzwerk

Deine Geräte sind Teil eines Netzwerks, welches Teil eines größeren Netzwerks ist, welches Teil eines sogar noch größeren Netzwerks sein kann, welches - du verstehst schon. Das ist das Internet, ein Netzwerk an Computernetzwerken, klein und groß. Und du bist ein Teil davon.

Das Netzwerk, das dir am nächsten ist, wird LAN genannt - Local Area Network. Es bezieht sich auf eine Gruppe von miteinander verbundenen Geräten an einem physikalischen Ort. Wenn du dich also mit deinem Router zu Hause verbindest, verbindest du dich mit deinem LAN.

Dein heimisches Netzwerk ist wahrscheinlich ziemlich klein, mit bis zu zehn verbundenen Geräten (oder wenn du Technik liebst, deutlich mehr - aber wir verurteilen dich nicht, Technik ist super). Ein LAN kann es auch in einem Unternehmen geben, oder es deckt die gesamte Schule ab mit tausenden miteinander verbundenen Geräten.

Verwandte Begriffe: Internet, LAN

P

Phishing

Du bekommst eine E-Mail von deiner Bank. Es handelt sich um eine Warnung: jemand hat versucht, Geld von deinem Konto abzuheben. „Bitte senden Sie UNVERZÜGLICH Ihr Login und Ihr Passwort, um Ihre Identität zu bestätigen“, schreibt die Bank.

Klingt beängstigend, aber aus Angst heraus solltest du nicht handeln.

Überprüfe den Absender sorgfältig, und du wirst wahrscheinlich feststellen, dass dieser nicht deine Bank ist, sondern jemand, der sich dafür ausgibt. Antworte darauf nicht, klicke auf keinen Link in der E-Mail. Rufe umgehend deine Bank an und frage nach der E-Mail.

Diesen Betrug nennt man Phishing, und er nimmt verschiedene Formen an. Nachrichten oder E-Mails, die Angst und Dringlichkeit nutzen, um vertrauliche Details zu erfahren. Eine gefälschte Webseite, die fast genauso wie die von deiner Universität aussieht. Gib dein Login und dein Passwort ein, und du übermittelst sie einem Betrüger.

Die Verteidigung ist einfach - sei vorsichtig. Achte auf verdächtige Nachrichten, die mit Angst spielen oder noch schlimmer - etwas versprechen, das zu gut ist, um wahr zu sein. Übrigens hast du einen Klick hier, um sie zu beanspruchen.

Atme durch, denke nach, und prüfe nochmal genau. Klicke nicht auf einen Link, wenn die URL nicht seriös aussieht. Als allgemeine Regel gilt: gib niemals ein Passwort ein oder preis, wenn du nicht absolut sicher bist, dass es sicher ist.

R

Ransomware

Du schaltest deinen Computer ein und - warte, was ist das? Der Bildschirm lädt nicht. Aber da ist eine Nachricht: „Deine Dateien wurden von der NarutoRun Hacker Group verschlüsselt. Du hast eine Woche, um 500 US-Dollar in unser Wallet zu überweisen, oder deine Dateien sind für immer verloren. Rasengan!“

Klingt wie die Handlung einer schlecht geschriebenen Comedy, aber es ist nicht zum Lachen. Ransomware ist eine Art der Malware, die die Daten des Opfers zwangsweise verschlüsselt. Kein Mensch außer dem Hacker kann die Verschlüsselung rückgängig machen, weil nur er den Schlüssel besitzt (Es gibt Unmengen an Verschlüsselungsprotokollen, die ohne den Entschlüsselungsschlüssel praktisch nicht zu knacken sind).

Du solltest das Lösegeld nicht zahlen, weil dein Geld (wahrscheinlich in Form einer Kryptowährung von den Hackern gefordert) nur Kriminelle unterstützt. Lerne stattdessen, wie du dich gegen Ransomware schützt:

- Lade nichts von verdächtigen Webseiten herunter. Öffne keine verdächtigen Links, E-Mails oder Nachrichten. Siehe: Phishing.
- Erstelle ein Backup deiner sensibelsten Daten
- Update deine Apps und deine Software, vor allem deine Sicherheitssoftware
- Verwende starke Passwörter

S

Social engineering

Du wirst am frühen Morgen von deinem Smartphone geweckt. Die Person am anderen Ende erklärt freundlich, dass er ein Techniker bei LiteNet ist, deinem Internetanbieter. Es gab einen Netzwerkfehler, der zu kleineren Datenverlusten geführt haben könnte.

Könntest du bitte zum Datenabgleich deine Adresse und dein Geburtsdatum bestätigen?

Noch im Halbschlaf gibst du die Daten durch und kehrst zurück zu deinen Träumen. Du wachst zwei Stunden später ausgeschlafen auf, genehmigst dir ein riesiges Frühstück und findest heraus, dass du gehackt wurdest.

Die Person, die dich angerufen hat, war kein Techniker, sondern ein Social Engineer - ein Betrüger, der psychologische Manipulation einsetzt, um Leute auszutricksen, und sie dazu bringt, eine bestimmte Aktion auszuführen oder sensible Details preiszugeben.

Schauen wir uns das nochmal an. Der Betrüger erwischte dich früh am Morgen, stellte sich vor, um deinen Verdacht zu zerstreuen (LiteNet ist der größte Internetanbieter in deiner Gegend, das war einfach), und nannte ein paar bedeutungslose technische Begriffe, um seriös zu klingen.

Dann rief er LiteNet an, um sich als Du auszugeben und sagte, dass er sein Passwort vergessen hätte. Er gab dein Geburtsdatum und die Adresse an, um die Identität zu bestätigen (genauer gesagt: deine Identität), und setzte sein LiteNet-Passwort zurück - einschließlich des Passworts für dein E-Mail-Konto bei LiteNet.

LiteNet als Internetanbieter gibt es nicht wirklich; wir haben ihn für diese Geschichte erfunden. Dein Geburtsdatum und Adresse können genutzt werden, um Deine Passwörter zu knacken oder zurückzusetzen. Wenn du dich anmeldest, solltest du so wenige sensible Informationen wie möglich weitergeben, und ausdrücklich über das Telefon keine Details an- und weitergeben.

Social Engineers verwenden viele Techniken, um Nutzer zu manipulieren, ausgeklügelt und unverblümt. Ein Betrüger kann tausende an gefälschten E-Mails verschicken in der Hoffnung, ein paar Opfer zu finden, die naiv genug sind, mit ihren Kreditkartendetails oder Passwörtern zu antworten. Siehe auch: Phishing.

T

Zwei-Faktor-Authentifizierung

Du loggst dich auf dem Smartphone eines Freundes bei Twitter ein, weil du deins zu Hause gelassen hast. Da es sich um ein neues Gerät handelt, musst du den Login in einer speziellen App zur Authentifizierung bestätigen. Diese befindet sich auf deinem Smartphone. Welches zu Hause ist.

Verflixt, das ist ein Cybersicherheit-Dilemma!

Ja, es kann ein wenig lästig für dich sein, aber die Zwei-Faktor-Authentifizierung (2FA) sichert dich mit einer zweiten Schutzschicht ab. Wenn du ohne dein Smartphone Probleme hast, auf dein Konto zuzugreifen, dann haben das auch die Hacker.

Die zwei Faktoren sind normalerweise:

Etwas, das du kennst (ein Passwort oder ein PIN-Code). Etwas, das du hast (ein Smartphone, ein Codebuch oder deine biometrischen Daten).

Kein System ist unüberwindlich, aber 2FA verbessert die Sicherheit deiner Konten auf ein Level, das über das der meisten Nutzer hinausgeht. Cyberkriminelle sind in der Regel opportunistisch; statt also einen Weg zu finden, um 2FA zu umgehen, suchen sie sich andere Ziele, vorzugsweise eine Person, die ABCDEFG als ihr Passwort verwendet.

Du solltest 2FA bei allen Diensten aktivieren, die es unterstützen. Es ist eine einfache Möglichkeit, mit minimalen Unannehmlichkeiten online sicherer unterwegs zu sein.

Verwandte Begriffe: Multi-Faktor-Authentifizierung

V

VPN

Du stöberst online, scrollst, surfst. Und jedes Mal, wenn du online bist, hinterlässt du kleine Datenspuren von dir. Dein Internetanbieter hat Zugang zu deinem Online-Verkehr. Jede Webseite, die du besuchst, kann deine IP-Adresse sehen.

Es geht nicht nur um Privatsphäre, sondern deine Online-Sicherheit steht auch auf dem Spiel. Viele Webseiten nutzen kein sicheres Kommunikationsprotokoll. Die meisten Anwendungen legen nicht offen, welche Maßnahmen zur Cybersicherheit sie verwenden. Du musst ihnen, ohne Beweise dafür zu haben, vertrauen.

Ein VPN (Virtuelles Privates Netzwerk) ist ein Tool, das deinen Datenverkehr durch einen sicheren Server leitet, ihn dabei verschlüsselt und deine IP-Adresse und deinen virtuellen Standort verändert. Selbst wenn es technisch klingen mag, ist ein VPN ein Tool, das auch für einen Laien leicht zugänglich ist.

Das bedeutet nicht, dass alle VPNs gleich gut sind. Ein VPN leitet all deine Daten durch seine Server, es kann also Daten sammeln und sie an den Höchstbietenden verkaufen. Die gute Nachricht ist, dass die meisten der größten VPNs transparent sind, was ihr Vorgehen angeht, keine Benutzerprotokolle speichern und damit nichts an Dritte verkaufen oder preisgeben können.
Wir bei NordVPN zum Beispiel haben unseren No-Logs-Grundsatz, der regelmäßig von einem der „Big-Four"-Wirtschaftsprüfungsgesellschaften überprüft wird.

Verwandte Begriffe: Zeitbombe, interne Bedrohung

W

WLAN

Du bist in einem Hotelzimmer und surfst über das kostenlose WLAN. Ein paar Etagen unter dir späht ein Hacker deine Online-Aktivität aus. Wie?

Ein öffentliches WLAN ist grundsätzlich unsicher - Cyberkriminelle können viele Methoden verwenden, um es auszunutzen oder zu kompromittieren.

Wenn der Router schlecht konfiguriert ist, könnte ein Hacker von jedem Nutzer des öffentlichen Hotspots den Internetverkehr verfolgen. Oder der Hacker kann einen Weg finden, um Schadsoftware über das Netzwerk in dein Gerät zu injizieren.

Ein Hacker kann einen gefälschten Hotspot einrichten - einen Evil Twin - und dich dazu bringen, dich damit zu verbinden: Siehe auch: Man-in-the-Middle-Angriff.
Wie sicher du bist, hängt von Folgendem ab:

Die Konfiguration und Sicherheitsmaßnahmen des Hotel-WLAN. Die Sicherheitspraktiken der Webseiten, die du besuchst, und der Apps, die du verwendest. Deine persönlichen Cybersicherheit-Praktiken.

Normalerweise kannst du nicht wissen, wie sicher ein öffentliches Netzwerk ist, vermeide also, auf sensible Daten zuzugreifen, wenn du dich damit verbindest. Wieso wechselst du nicht stattdessen zu mobilen Daten? Oder schaltest ein VPN an?

P.S.: Wenn du ein Event organisierst, verlasse dich nicht auf das WLAN des Veranstaltungsortes, denn das ist selten sicher. Die richtige Einrichtung eines WLAN-Hotspots ist keine leichte Aufgabe und erfordert präzises technisches Wissen - engagiere lieber Experten, wenn du nicht über die technischen Fähigkeiten verfügst.

Aber dein Job ist genauso wichtig - du musst kommunizieren! Informiere die Teilnehmer des Events über die offiziellen Hotspots und warne sie vor einer Verbindung mit anderen Hotspots, selbst wenn diese seriös wirken.

Verwandte Begriffe: Schadsoftware-Injektion, WLAN-Schnüffelei.

Z

Zero-Day-Exploit

Du hast deine Software aktualisiert, ein Antiviren-Programm installiert, deine Firewall eingeschaltet. In diesem Moment könnte sich kein Hacker in dein System hacken, oder?

Wenn es nur so einfach wäre.
Computernetzwerke, Software und Hardware werden von Menschen erstellt. Menschen machen Fehler, sie durchdenken nicht jedwedes Szenario, sie hinterlassen Schwachstellen.

Hacker nutzen diese aus. Sie suchen nach dem schwächsten Glied im System und brechen es.

Sobald eine Schwachstelle entdeckt wird, wird sie gepatcht. Die Updates, die du für deine Apps oder dein Betriebssystem installierst, sind das oft - Patches für neu entdeckte Schwachstellen.

(Natürlich können manche Schwachstellen nie gepatcht werden. Menschen, nicht Maschinen, sind oft das schwächste Glied, wenn es um Cybersicherheit geht. Siehe: Social Engineering.)

Eine Zero-Day-Schwachstelle ist dem Anbieter nicht bekannt, und deshalb wurde sie nicht gepatcht. Der Name bezieht sich auf die Anzahl an Tagen, die ein Anbieter Zeit hat, die Schwachstelle zu beheben - null (Englisch: zero). Eine Attacke, die auf dieser Schwachstelle basiert, wird Zero-Day-Exploit oder Zero-Day-Angriff genannt.

Selbst wenn du also dein System für sicher hältst, patchst und mit den neusten Updates versorgst, kann ein Zero-Day-Exploit es durch eine von vornherein unbekannte Schwachstelle kompromittieren. Die Lösung ist ständige Wachsamkeit. Sei klug, wenn du online bist, verwende starke Passwörter, klicke nicht auf Links, von denen du nicht weiß, ob sie sicher sind.

Auf diese Weise minimierst du deine Risiken und zwingst Cyberkriminelle dazu, sich nach leichteren Zielen umzusehen.

Verwandte Begriffe: Zero-Day-Schwachstelle, Zero-Day-Angriff