HISCOX
WISSEN VERSICHERT.

CYBER-GLOSSAR

HISCOX
WISSEN VERSICHERT.

Cyber-Glossar

Ad Blocker	Eine Browsererweiterung (Plugin/Extension), die verhindern soll, dass Werbung auf Websites angezeigt wird. Einige Ad Blocker beinhalten jedoch auch Spyware, umgehen somit den Datenschutz der Nutzer und werten gesammelte Daten aus.
Advanced persistent threat (APT)	Der Begriff bedeutet „Fortgeschrittene, andauernde Bedrohung“ und meint eine komplexe, zielgerichtete Attacke auf kritische IT-Infrastrukturen eines bestimmten Unternehmens oder einer bestimmten Organisation.
Agile Software-entwicklung	Die Programmierung von Software erfolgt durch Teams, die sich selbst organisieren. Bürokratische Regeln, die Programmierer aufhalten könnten, sollen damit ausgehebelt werden. Der Entwicklungsprozess läuft flexibler und schlanker ab als bei der konventionellen Art der Softwareentwicklung.
Anonymizer	Sammelbegriff für Lösungen, die Personen die unerkannte Nutzung von Onlinediensten ermöglichen. Häufig wird die Anonymität gewährleistet, indem zwischen besuchter Website und Nutzer ein weiterer Umweg (Server) über einen VPN-Tunnel in die Verbindung eingebaut wird. Jedoch werden auf diesen zwischengeschalteten Servern oft Verbindungsdaten (die jedoch von den Strafverfolgungsbehörden nicht herausgegeben werden) protokolliert. Dann ist keine komplette Anonymität gewährleistet. Wichtig ist in jedem Fall die Verschlüsselung (SSL/TLS), damit das Abhören der Verbindung zwischen Nutzer und Proxy verhindert wird.
API	Die Abkürzung für „Application Programming Interface“. Übersetzt bedeutet das „Programmschnittstelle“. Über ein API können Entwickler auf die Funktionen einer Anwendung zugreifen. So könnte man es vereinfacht ausdrücken: Wenn Software B automatisch Informationen von Software A abrufen und nutzen kann, dann handelt es sich bei der dafür notwendigen Schnittstelle um die sogenannte API. Dies verhindert in der Praxis Medienbrüche und Informationsverluste.
Autocomplete	Funktion zur Autovervollständigung für Computer und Smartphones. Dabei werden Vorschläge zur Vervollständigung des Wortes, das man gerade tippt, angezeigt. Früher bekannt als T9 auf Mobiltelefonen mit Tasten. Autocomplete kann lustige Sätze hervorrufen, wenn man bei der Nutzung nicht aufpasst und ein falsches Wort (versehentlich) bestätigt. **Es gibt Websites, die solche Konversationen publizieren.** Doch Vorsicht bei der Weitergabe von privaten Nachrichten in die Öffentlichkeit. Das Persönlichkeitsrecht des Absenders darf nicht verletzt werden – sonst drohen rechtliche Konsequenzen.
Backdoor	Bildlich gesprochen: Eine Hintertür, um sich Zugang zu einem geschützten Bereich zu verschaffen. Man geht also nicht durch die gesicherte und verschlossene Haustür, sondern geht einmal um das Haus herum und kommt herein beziehungsweise bricht ein. In Kombination mit einem Trojaner (s. Erklärung Trojaner) verschaffen sich Cyberkriminelle Kontrolle über schlecht gesicherte PCs, Server, Smartphones oder sonstige mit dem Internet verbundene Geräte. Programmierer müssen also darauf achten, dass sie Sicherheitslücken entfernen, damit dieses verhindert wird. Beispiel: **Magento Onlineshop mit veralteter Software**
Backup	Eine Datensicherung oder Backup ist eine Kopie aller gespeicherten Daten mit dem Ziel, diese im Fall eines Datenverlustes (wie der Löschung oder Verschlüsselung) wiederherstellen zu können.
Blacklist	Eine Liste mit IP-Adressen oder Mail-Adressen, denen der Zugang zu IT-Systemen verweigert oder nur eingeschränkt möglich ist.
Blockchain	Eine Blockchain ist eine geteilte, öffentliche, verschlüsselte Datenbank. Die gemeinsam genutzte Datenbanktechnologie verknüpft Verbraucher und Lieferant einer Transaktion direkt miteinander.
Botnetz	Zusammenschluss von mehreren Bots (abgeleitet von Robotern), die zentral gesteuert werden. Bots sind automatisierte Schadprogramme die meist ohne Kenntnis und Erlaubnis des Besitzers auf mit dem Internet verbundene Geräte installiert sind (Internet of Things, wie Smart Home Leuchtmittel, Kühlschränke, Kameras etc..) Diese werden genutzt, um gleichzeitig gezielt eine Webanwendung anzufragen um diese zu überlasten (Distributed Denial of Service Angriff).

HISCOX
WISSEN VERSICHERT.

Cyber-Glossar

Business E-Mail Compromise	Business E-Mail Compromise geschieht über ein internes E-Mail-Konto des Unternehmens, zu dem sich ein Hacker Zugang verschafft hat (in der Regel geschieht dies über eine Phishing E-Mail, mit der Zugangsdaten und Passwörter erbeutet werden). So lassen sich Kunden oder Mitarbeiter des Unternehmens leicht täuschen, da die Informationen von einer scheinbar vertraulichen Quelle stammen.
Chatbot	Programm, das automatisch Textnachrichten oder auch gesprochene Sätze beantwortet. Man findet sie in Apps für private Nachrichten (WhatsApp, Facebook, Messenger, …) und in Chatsystemen. Die Bots sollen beispielsweise den Kundendienst entlasten, da sie Antworten auf häufig gestellte Fragen geben können. **Unser Artikel über Chatbots.**
Cyber Mobbing	Cyber Mobbing umfasst alle Arten von Verleumdung, Belästigung, Bedrängung und Nötigung über das Internet und elektronische Medien wie Chat-Rooms, Messenger Dienste oder Social Media.
Cybersecurity / Cybercrime	Computersicherheit und Computerkriminalität stehen in einem engen Context zueinander. Ist der Computer geschützt, kann der Kriminelle nur schwer an die Daten heran. Wird ein nicht hinreichend gesicherter Computer angegriffen, kann ein großer Schaden entstehen. Cyber-Kriminelle fangen Daten ab und verschaffen sich Zugang zu Systemen, sodass der Nutzer zudem noch finanziellen Schaden erleidet.
Cyberspace	Als Cyberspace bezeichnet man jede nicht real aber virtuell existierende Welt, die mit einem Computer „betreten“ werden kann. Sie soll eine nahezu perfekte Illusion räumlicher Tiefe und realitätsnaher Bewegungsabläufe sein.
DoS- und DDoS-Attacke	Eine künstlich herbeigeführte Überlastung eines Webservers oder Datennetzes – gesteuert von Cyber-Kriminellen. Im Gegensatz zu einer einfachen Denial-of-Service-Attacke (DoS) haben Distributed Denial-of-Service-Attacken (DDoS) eine immense Schlagkraft. Mehrere Computer greifen dabei gleichzeitig und im Verbund (Botnetze) eine Webseite oder eine ganze Netzinfrastruktur an. Dies kann sehr schnell zum Ausfall der Server führen. Beispiel: **DDoS-Attack gegen Zahlung von BitCoins abwehren**
Doxing	Doxing ist das internetbasierte Zusammentragen und Veröffentlichen personenbezogener Daten, zumeist mit bösartigen Absichten gegenüber den Betroffenen. Gründe können zum Beispiel Selbstjustiz, öffentliches Bloßstellen sowie Belästigung sein.
Hashwert	Der Hashwert ist eine Prüfsumme und spielt bei der Verschlüsselung von Passwörtern und Nachrichten eine wichtige Rolle, da er keine Rückschlüsse auf den Inhalt zulässt. Der Hashwert wird häufig auch als digitaler Fingerabdruck bezeichnet.
HTTPS und SSL / TLS	HyperText Transfer Protocol Secure (HTTPS, englisch für „sicheres Hypertext-Übertragungsprotokoll“) ist ein Protokoll im World Wide Web, um Daten abhörsicher zu übertragen. Transport Layer Security (TLS, deutsch Transportschichtsicherheit) ist ein hybrides Verschlüsselungs-protokoll zur sicheren Datenübertragung im Internet. Secure Sockets Layer (SSL) ist umgangssprachlich bekannter, jedoch veraltet und die Vorgängerbezeichnung für das besagte Protokoll. **Mehr Informationen zu verschlüsselten Webseiten in unserem Artikel.**
Kryptojacking	„Cryptojacking“ setzt sich aus den englischen Begriffen „Cryptocurrency“ (Kryptowährung) und „Hijacking“ (Entführung) zusammen. Gemeint ist die Übernahme der Rechenleistung eines Dritten mit dem Ziel, diese für das Schürfen digitaler Kryptowährungen zu missbrauchen.
Kryptomining	Beim Kryptomining wird Rechenkraft genutzt, um Kryptowährungen wie Bitcoin, Monero oder Ethereum zu schürfen. Der Begriff kommt aus dem Bergbau – das (Gold-)Schürfen wurde zum Namensgeber und macht einen Intermediär wie zum Beispiel eine Bank überflüssig.
Kryptowährung	Kryptowährungen wie Bitcoin sind unabhängige digitale Zahlungsmittel. Als Zahlungssystem sollen sie unabhängig und sicher sein.
Malware	Als Schadprogramm, Schadsoftware oder Malware (aus malicious „bösartig“ und Software) – bezeichnet man Computerprogramme, die entwickelt wurden, um unerwünschte oder schädliche Funktionen auszuführen z.B. Viren, Würmer, Trojaner oder Spyware.

HISCOX
WISSEN VERSICHERT.

Cyber-Glossar

Phishing	Phishing bezeichnet die illegale Methode, über gefälschte Webseiten, per E-Mail oder Kurznachrichten persönliche Daten oder Anmeldedaten von Internetnutzern abzugreifen. Die Daten eines Benutzers werden dann für betrügerische Aktionen genutzt. Mehr Informationen: **Scam wird immer besser – Vorsicht Falle**
Ransomware	Ein Angriff auf den eigenen Computer per schädlicher Software (Malware), die bösartig eingeschleust wurde. Die Malware sorgt dafür, dass der Computer infiziert wird und die Dateien auf der Festplatte und auf beschreibbaren Laufwerken verschlüsselt werden. Der Cyberkriminelle verlangt meist Geld (BitCoins) dafür, dass dieser Vorgang von ihm rückgängig gemacht wird (Entschlüsselung).
Risk Audit	Der Begriff bezeichnet eine Risikoprüfung (meist in Form eines Interviews) der IT-Infrastruktur mit dem Ziel, die Effektivität aller Sicherheitsmaßnahmen zu beurteilen.
Silent Cyber	Cyberrisiken, die Schäden in anderen Sparten als der reinen Cyberversicherung verursachen können.
Social Engineering	Der Begriff „Social Engineering“ bezeichnet eine Vorgehensweise, bei dem die Hilfsbereitschaft oder Gutgläubigkeit des „Faktor Mensch“ ausgenutzt wird. Zum Beispiel werden Mitarbeiter eines Unternehmens überzeugt, Sicherheitsvorkehrungen zu umgehen und sicherheitsrelevante Informationen preiszugeben.
Spear-Phishing	Bei Spear-Phishing handelt es sich um konkrete Angriffe auf natürliche Personen in Organisationen, um Zugriff auf vertrauliche Daten wie Geschäftsgeheimnisse oder Finanzinformationen zu erhalten. Im wörtlichen Sinne (spear = Speer) wird gezielt nach Daten gefischt und nicht großflächig mit einem Schleppnetz.
Spyware	Im Gegensatz zu Computerviren, die sich weiterverbreiten, ist Spyware ein Programm auf dem Rechner, das sich fest eingenistet hat. Meist dienen Spyware-Programme dazu, das Nutzungsverhalten, insbesondere das Surfverhalten im Internet, auszuspähen (spy = spähen). Die gewonnenen Daten werden kommerziell verwertet.
Trojaner	Als Trojaner bezeichnet man ein Computerprogramm, das gezielt in fremde Computer eingeschleust wird, um dort Schaden anzurichten. Es ist als sinnvolles Programm getarnt, versteckt jedoch zerstörerische Funktionen. Beispiel: Krypto-Trojaner Locky
Zwei-Faktor-Authentifizierung	Bei einem Login mit der Zwei-Faktor-Authentifizierung (2FA) benötigt man – neben dem Benutzernamen und Passwort – noch eine weitere eindeutige Information. Oft ist das eine zusätzliche Ziffernfolge. Per App oder SMS wird der Einmalcode auf Anforderung gesendet. So kann der Zugriff auch Accounts mit geleakten Passwörtern und Zugangsdaten verhindert werden. Mehr Info in unserem Artikel **Zwei-Faktor-Authentifizierung.**

Sie möchten mehr zum Thema Cyberrisiken erfahren? Dann besuchen Sie uns online:

Cyber-Informationen für Endkunden
Cyber-Informationen für Makler
Kostenloses Cyber-Training
Business Blog Cyber & IT

Hiscox
Arnulfstraße 31, 80636 München
T +49 89 54 58 01 100
E hiscox.info@hiscox.de