Deutsche Leukämie- & Lymphom-Hilfe
Bundesverband der Selbsthilfeorganisationen zur Unterstützung von Erwachsenen mit Leukämien und Lymphomen e.V.

Wegweiser für sicheres Surfen im Internet nicht nur für Leukämie- und Lymphom-Betroffene

Holger Bassarek, Dipl.-Ing. (FH), DLH-Webmaster und DLH-Vorstandsmitglied

[Erläuterungen zu Fachbegriffen und Abkürzungen siehe Textende]

Die tägliche Nutzung des Internets ist für einen Großteil der Bevölkerung heutzutage selbstverständlich. Kommunikation, Informationsfindung, Präsentation und geschäftliche Transaktionen finden in einem immer stärkeren Maße online statt. Im Internet kann man sich jederzeit informieren und mit Anderen Kontakt aufnehmen. Bezüglich der Selbsthilfe zeigen sich hier viele Ähnlichkeiten zwischen einer normalen Selbsthilfegruppe und dem Austausch im World Wide Web (WWW). Die Fülle an Seitenanbietern und Informationen macht es aber auch schwer, das gewünschte und dazu noch seriöse Angebot herauszufiltern. Gibt man bei gängigen Suchmaschinen z.B. das Stichwort „Leukämie“ ein, erhält man weit über fünf Millionen Ergebnisse. Gefunden werden hier allerdings nicht nur gute und seriöse, sondern auch veraltete oder schlichtweg falsche Informationen. Auch gibt es Anbieter, die unkonventionelle oder sogar illegale Produkte anbieten. Die Schwierigkeit ist es, aus diesem riesigen Angebot gute Informationen herauszufiltern. Hier sollten Sie sich ein paar Verhaltensregeln zur Nutzung und Informationssuche im Internet zu eigen machen.

Suche im Internet

Webseiten von relevanten Organisationen

Ein erster und einfacher Einstieg in die Internetrecherche ist der Besuch von Webseiten themenbezogener und seriöser Organisationen. Beispiele dafür sind die Seiten der Deutschen Leukämie- & Lymphom-Hilfe, der Deutschen Krebshilfe und des Krebsinformationsdienstes (KID). Hier können Sie erste interessante Informationen zur Thematik finden, wie z.B. Ratgeber, Infoblätter oder weiterführende Links.

Die Internetadressen dieser Webseiten setzen sich meistens aus Bestandteilen des Namens dieser Organisationen zusammen, wie z.B. www.leukaemie-hilfe.de für die Seite der Deutschen Leukämie- & Lymphom-Hilfe. Da sich die exakte Zusammensetzung der Adresse jedoch von Organisation zu Organisation unterscheidet, muss man des Öfteren auf eine andere Art der Suche zurückgreifen: die Suche über Suchmaschinen.

Verwendung von Suchmaschinen

Die schnellste und einfachste Methode zur Suche im Internet ist die Nutzung einer Suchmaschine. Suchmaschinen bieten die Möglichkeit, über Stichwörter Anbieter und Infos im Internet zu finden.

Die Suchmaschinen bestehen aus Datenbanken, in denen die Adressen der einzelnen Internet-Seiten mit den Suchbegriffen und teilweise mit kurzen Beschreibungen abgespeichert sind (Indexierung). Die Internet-Seiten werden entweder direkt vom Anbieter

bei den entsprechenden Suchbrowsern online eingetragen oder die Suchmaschine durchforstet das Internet mit Robots (automatische Suchroutinen) nach neuen oder aktualisierten Internet-Seiten.

Nach Eingabe des Suchbegriffs liefert die Suchmaschine eine Liste von Verweisen auf Dokumente, meistens dargestellt mit Titel und kurzem Auszug des jeweiligen Dokuments. Die Sortierung erfolgt nach Relevanz oder/und teilweise nicht leicht zu durchschauenden Kriterien der Suchmaschinenanbieter sowie Werbeanzeigen und sollte deswegen keinesfalls als ausschließliche Gütebewertung gesehen werden.

Die Kunst der Nutzung einer Suchmaschine besteht darin, das Suchergebnis zu verfeinern. So können verschiedene Suchmaschinen unterschiedliche Arten von Daten durchsuchen. Zunächst lassen sich diese grob in die „Dokumenttypen“ wie Text, Bild, Ton, Video und andere unterteilen. Suchanfragen sind oft mehrdeutig und damit unpräzise. So kann die Suchmaschine nicht selbstständig entscheiden, ob beim Begriff „Laster“ nach einem LKW oder einer schlechten Angewohnheit gesucht werden soll. Umgekehrt sollte die Suchmaschine nicht zu stur auf dem eingegebenen Begriff bestehen. Sie sollte auch Synonyme einbeziehen, damit z.B. beim Suchbegriff „Rechner Windows“ auch Seiten gefunden werden, die statt Rechner das Wort Computer enthalten.

Tipp: Verwenden Sie die bei den meisten Suchmaschinen angebotene „Erweiterte Suche“, um das Suchergebnis einzugrenzen.

Trotzdem bleibt einem nichts Anderes übrig, als sich mehrere Seiten aus der Ergebnisliste anzuschauen, um die Brauchbarkeit festzustellen.

Beispiele für gebräuchliche Suchmaschinen

(Suchmaschinen, die nicht tracken)
www.duckduckgo.com
www.gibiru.com
www.startpage.com

(Suchmaschinen, die tracken)
www.bing.de
www.fireball.de
www.google.de
www.lycos.de
www.yahoo.de
www.web.de

Einstieg über Portale
Eine andere Möglichkeit der Recherche ist der Einstieg über sogenannte Portale. Im Bereich Medizin gibt es im Internet einige Gesundheitsportale, die gesundheitsrelevante Informationen enthalten oder über Links auf thematisch relevante Seiten verweisen.

Beispiel:
Krebsinformationsdienst: www.krebsinformationsdienst.de

Man sollte jedoch beachten, dass jedes Gesundheitsportal von einer bestimmten Interessengruppe betrieben wird und die Inhalte entsprechend ausgerichtet sind. Um die Seriosität des Anbieters zu überprüfen, werfen Sie einen Blick auf das Impressum, welches auf den Betreiber der Seite hinweist.

Abonnieren von Newslettern
Auch Newsletter sind eine Möglichkeit, sich Informationen aus dem Internet zu holen, indem man sich mit seiner E-Mail-Adresse in einen Verteiler einträgt. Zum allgemeinen Thema Krebs gibt es zahlreiche, für Leukämien und Lymphome wenige deutschsprachige Angebote.

Teilnahme an Diskussionsforen
Diskussionsforen haben den Vorteil, dass man zeitversetzt diskutieren kann. Eine Frage oder ein Bericht wird gespeichert, und andere Leser können zu einer beliebigen anderen Zeit darauf antworten. Die Wahrscheinlichkeit, einen passenden Gesprächspartner zu finden, ist dadurch viel größer - auch weil die Beiträge wieder durch Suchmaschinen gefunden werden können.

Beispiele:
Forum der Deutschen Leukämie- & Lymphom-Hilfe: forum.leukaemie-hilfe.de
Forum von Leukämie-Phoenix: forum.leukaemie-phoenix.de
Forum der AMM online (Arbeitsgemeinschaft Multiples Myelom): www.myelom.org/forum

Soziale Netzwerke
Soziale Netzwerke sind Plattformen, die mit Werkzeugen zur Kommunikation (z.B. Chat, Foren, Instant-Messenger) den Austausch zwischen Internetnutzern ermöglichen (z.B. Facebook). Oft ist hier allerdings die Transparenz der Anbieter und der Datenschutz nicht in genügendem Maße gewährleistet.

Fachmagazine
Verschiedene thematisch relevante Fachmagazine stellen ihre Informationen (teilweise eingeschränkt) auch im WWW zur Verfügung. Bei diesen Angeboten kann man von einer hohen Qualität der Informationen ausgehen. Viele Online-Fachmagazine bieten die Möglichkeit, sich Artikel nach selbst festgelegten Suchkriterien per E-Mail zusenden zu lassen (siehe auch „Abonnieren von Newslettern“).

Beispiele:
Ärzte-Zeitung: www.aerztezeitung.de
Deutsches Ärzteblatt: www.aerzteblatt.de

Überprüfung der Qualität von Internetseiten
Für die Informationssuche und den Austausch im Internet (und nicht nur da) sollten Sie sich folgende Regeln zur Nutzung und Überprüfung der Qualität zu eigen machen.

a) Gegenprobe
Überprüfen Sie die medizinischen Informationen aus dem Netz mindestens bei einem zweiten Web-Angebot.

b) Foren und Soziale Netzwerke
Foren und Soziale Netzwerke können dem persönlichen Erfahrungsaustausch dienen. Fachliche Qualität ist hier nicht garantiert. Ausnahmen bilden eventuell von Experten moderierte Chats und Foren.

c) Misstrauen
Sensationelle Heilsversprechen sollten Sie misstrauisch machen.

d) Kein Ersatz
Das Internet kann helfen, einen Arztbesuch vor- und nachzubereiten oder Informationen zu finden. Einen Arztbesuch ersetzen kann es nicht.

e) Qualitätssiegel
Es gibt Qualitätssiegel für Gesundheits-Webseiten. Das bekannteste deutsche Qualitätssiegel ist das afgis Qualitätslogo (www.afgis.de). Ein anderes deutsches Qualitätslogo ist „medisuch“ (www.medisuch.de). Trägt eine Webseite eines dieser Logos, wurden festgelegte formale Kriterien von unabhängiger Seite überprüft. Qualitätssiegel sagen allerdings in der Regel nichts über die sachliche Richtigkeit der Inhalte aus.

f) Checkliste
So prüfen Sie die Qualität von medizinischen Angeboten im Netz:

- Ist der Anbieter einer Internetseite leicht zu erkennen?
- Sind der Zweck und die Zielgruppe einer Seite genannt?
- Sind Autoren und Quellen der Informationen aufgeführt?
- Sind Alter und Aktualität der Informationen angegeben?
- Besteht die Möglichkeit, mit dem Anbieter (per E-Mail, Telefon oder Post) in Kontakt zu treten?
- Ist Werbung als solche gut erkennbar und von der Information getrennt dargestellt?
- Werden Angaben über die Finanzierung (und damit mögliche finanzielle Interessen) und Sponsoren gemacht?
- Können Nutzer erkennen, ob und wenn ja, welche ihrer Daten beim Besuch der Internetseite gespeichert und wie diese ggf. weiterverwendet werden?
- Sind Informationen verständlich und übersichtlich dargestellt?
- Werden vorgeschlagene Therapien genau beschrieben?
- Werden Vor- und Nachteile der Therapie genannt?
- Gibt es Hinweise auf weitere Untersuchungen und Behandlungsmöglichkeiten?
- Gibt es Hinweise auf weiterführende Quellen?
- Werden alle Fragen zum Thema beantwortet?

Beispiele guter Webseiten für Leukämie- und Lymphom-Betroffene

- **Deutsche Leukämie- & Lymphom-Hilfe e.V. (DLH)**
  www.leukaemie-hilfe.de
  Hier haben Sie u.a. Zugriff auf die INFO-Blätter der Organisation, um sich zu den verschiedenen Leukämien und Lymphomen informieren zu können. Auch gibt es eine Übersicht der relevanten Selbsthilfegruppen. Empfehlenswert ist der Punkt „Literaturliste“, der Buchtitel nennt oder Broschüren zum Herunterladen anbietet. Insgesamt finden Sie hier ein vielfältiges, umfangreiches Angebot.

- **Deutsche Krebshilfe**
  www.krebshilfe.de
  Nach dem Motto „Helfen. Forschen. Informieren." fördert die Organisation Projekte zur Verbesserung der Prävention, Früherkennung, Diagnostik, Therapie, medizinischen Nachsorge und psychosozialen Versorgung einschließlich der Krebs-Selbsthilfe. Die Deutsche Krebshilfe informiert die Bevölkerung über das Thema Krebs und die Möglichkeiten, Krebs zu vermeiden und früh zu erkennen.

- **Deutsche Krebsgesellschaft**
  www.krebsgesellschaft.de
  Die Deutsche Krebsgesellschaft berät Betroffene, Interessierte und Ärzte. Sie bietet Informationen zu den Themen Vorbeugung und Früherkennung sowie die Darstellung einzelner Krankheitsbilder. Wechselnde Aktionen wie Live-Sprechstunden oder Aktionstage sowie die Vorstellung des Beratungsnetzes in Deutschland sind besondere Services dieser Seite.

- **Kompetenznetz Maligne Lymphome**
  www.lymphome.de
  Führende deutsche Forschungsgruppen und Einrichtungen arbeiten in diesem Kompetenznetz zusammen. Ziel ist es, das Wissen zu bündeln und Forschungsergebnisse schneller in die Patientenversorgung zu übertragen. Ärzte und Patienten finden aktuelle Informationen.

- **German Lymphoma Alliance (GLA)**
  https://www.german-lymphoma-alliance.de/
  Die GLA hat sich zum Ziel gesetzt, die Therapieergebnisse für Lymphom-Patienten in Deutschland nachhaltig zu verbessern. Im Bereich „Studien" findet sich eine Übersicht der laufenden Studienprojekte. Im Bereich „Patienten" kann man sich für einen Newsletter anmelden.

- **Projekt „Leukämie- und Knochenmark-/ Stammzelltransplantation**"
- www.leukaemie-kmt.de
  Hier finden Sie für das Internet aufbereitete, für den Laien leicht verständliche Informationen zur Thematik Leukämie und Knochenmark-/Stammzelltransplantation. Gepflegt wird die Seite von einem Betroffenen.

- **Leukämie-Online e.V.**
  www.leukaemie-online.de
  Eine Wissensdrehscheibe einer Online-Gemeinschaft - von Betroffenen für Betroffene. Hier gibt es eine Fülle an brauchbaren Hinweisen, Foren, etc..

- **Haarzell-Leukämie-Hilfe e.V.**
  www.haarzell-leukaemie.de
  Hier finden Sie Erstinformationen für Haarzell-Leukämie-Neubetroffene, Informationen über Behandlungsmethoden, Kontakte zu Spezialisten/Fachleuten und Möglichkeiten des Erfahrungsaustausches.

- **Leukämie-Phoenix**
  www.leukaemie-phoenix.de
  Leukämie-Phoenix versteht sich als „virtuelle Selbsthilfegruppe" für Patienten nach Leukämie-Behandlung (mit dem Schwerpunkt nach Stammzell-/Knochenmarktransplantation) und wird von einem Betroffenen betrieben.

- **Deutsche Knochenmarkspenderdatei gemeinnützige GmbH**
  www.dkms.de
  Auf dieser Seite geht es um alle Aspekte zu der Thematik Stammzellspende, von Hintergrundinformationen zu Leukämie, öffentlichkeitswirksamen Aktionen über Spendenaufrufe und -gesuche bis hin zu weiterführenden Links wie z.B. auf Selbsthilfegruppen etc. Alle können hier wichtige Informationen finden: Spender, Patienten, Ärzte, Schulen, Vereine, Firmen.

- **Betanet**
  www.betanet.de
  Hier können umfassende Informationen zu sozialmedizinischen und sozialrechtlichen Fragen recherchiert werden.

- **DocCheck Flexikon**
  flexikon.doccheck.com
  Das Flexikon ist ein offenes medizinisches Lexikon. Jeder registrierte DocCheck-User kann „medmachen" und Artikel kontrollieren, korrigieren, ergänzen oder neu erstellen.

- **Krebsinformationsdienst des dkfz**
  www.krebsinformationsdienst.de
  Hier findet sich umfassendes, aktuelles Wissen rund um Krebserkrankungen. Erwähnenswert ist insbesondere im Bereich „Service – Adressen und Links" die Suchmöglichkeit nach nächstgelegenen Krebsberatungsstellen und Psychoonkologie-Praxen.

- **BNHO e.V.**
  www.bnho.de
  Informationen des Berufsverbands der Niedergelassenen Hämatologen und Onkologen in Deutschland mit Adressenverzeichnis

Schutz im Internet

Verbindet man seinen Rechner mit dem Internet, setzt man ihn gewissen Risiken aus (z.B. dem Befall durch unerwünschte Schadprogramme). Deswegen sollten zwingend gewisse Schutzmaßnahmen getroffen werden.

Verwendung eines Virenschutzprogrammes
Auf jedem Rechner sollte ein Virenschutzprogramm installiert sein. Diese Programme arbeiten im Hintergrund und überprüfen ein- und ausgehende Daten sowie die lokalen Datenträger nach Computerviren, Spyware und anderer Schadsoftware. Das Vorhandensein eines Virenschutzprogrammes bietet allerdings keinen 100%igen Schutz. Damit es zuverlässig arbeiten und vor neu auftretenden Gefahren schützen kann, sollte es ständig aktualisiert werden. Es gibt inzwischen eine Vielzahl von Virenschutzprogrammen in unterschiedlichster Preis- und Leistungskategorie. Einige Betriebssystem-Anbieter bieten kostenlose Schutzprogramme an (z.B. Microsoft Defender).

Verwendung einer Firewall
Mit Firewall ist hier eine Software gemeint, welche den Datenverkehr zwischen dem eigenen Computer und dem Internet kontrolliert und regelt. Sie soll verhindern, dass Programme auf dem eigenen Rechner unautorisiert auf das Netz zugreifen und unberechtigte Zugriffe aus dem Netz auf den eigenen Rechner stattfinden. Es gibt kostenlose und kostenpflichtige Angebote. Die meisten Computer-Betriebssysteme beinhalten schon standardmäßig eine Firewall.

Durchführen von System- und Programmupdates
Wichtig für den störungsfreien Betrieb eines Rechners und das zeitnahe Schließen von Sicherheitslücken im System ist die Installation von aktuellen System- und Programmupdates. Für viele Betriebssysteme und Programme werden regelmäßig Updates zur Verfügung gestellt, die man schnellstmöglich installieren sollte. Update-Funktionen sollten regelmäßig und in kurzen Zeitabständen aufgerufen werden. Oft lässt sich die Updatefunktion von Betriebssystemen und Programmen in den Einstellungen automatisieren.

Schutz vor Phishing (Datendiebstahl)
Unter Phishing versteht man den Versuch, über gefälschte Internetseiten, E-Mails oder Kurznachrichten persönliche Daten eines Internetbenutzers zu erlangen, um diese dann missbräuchlich (z.B. Kontozugriff) zu verwenden. Oft werden dazu vertrauenswürdige Seiten gefälscht. Mit Phishing-E-Mails wird versucht, den Nutzer auf diese Seiten zu leiten.
Woran erkennt man Phishing-E-Mails?

- Merkwürdige Absenderadresse
- Eigene Adresse steht nicht im An-Feld
- Unpersönliche Anrede
- (Zeit)Druck wird aufgebaut („sie müssen sofort … sonst …“)
- Vertrauliche Daten wie PIN, TAN, Benutzername, Passwort werden abgefragt
- Schlechtes Deutsch, viele Rechtschreibfehler, fehlende Umlaute
- Links auf Seiten ohne https oder mit fehlerhaftem Zertifikat oder allgemein auf URL‘s, die nichts mit dem angeblichen Absender zu tun haben
- Keine ordentliche Signatur in der Nachricht
- Kein seriöses Unternehmen wird Ihnen jemals eine Rechnung o. ä. im Format DOC, XLS, PPT senden (sondern: PDF)

Auf jeden Fall sollte man ein gesundes Misstrauen gegenüber dem unsicheren Medium E-Mail entwickeln und E-Mails aufmerksam lesen. Prüfen Sie, ob der Absender seriös ist, bevor Sie eine in einer E-Mail verlinkte Internetseite aufrufen, einen E-Mail-Anhang öffnen oder in einer Antwort persönliche Daten mitteilen.

Verwendung sicherer Passwörter
In der Computerwelt findet Authentifizierung (z.B. bei Foren, Online-Shops, etc.) in der Regel durch Eingabe von Benutzernamen in Verbindung mit Passwörtern statt.

Um sich vor Missbrauch von Passwörtern durch Dritte zu schützen, sollte man einige Regeln beachten.

- Wahl eines sicheren Passwortes: Ein Passwort sollte möglichst lang sein, aus Buchstaben (Groß- und Kleinschreibung), Zahlen und Sonderzeichen bestehen. Es sollte kein sinnvolles Wort sein. Als Merkhilfe bieten sich Sätze an (z.B. mit dem Satz "**U**nsere **F**irma **k**auft **5**0 **% a**ller **L**ebensmittel **u**nter **1**0 **€ e**in**!**" kann man sich das Passwort "UFk5%aLu1€e!" merken).
- Für unterschiedliche Anwendungen sollten unterschiedliche Passwörter gewählt werden.
- Ein Passwort sollte nicht einfach so zu erraten sein und nicht in dieser Form in einem Wörterbuch zu finden sein. Ebenso sollte es nicht mittels Social Engineering herauszufinden sein (Name der Katze, Heimatort usw.).
- Es empfiehlt sich, Passwörter in regelmäßigen Abständen zu ändern.
- Passwörter sollten nicht aufgeschrieben oder unverschlüsselt gespeichert werden.
- Es empfiehlt sich Passwörter in einem Passwort-Manager abzulegen. Notwendig ist dann nur noch das Merken eines einzelnen (Master-)Passworts. Es gibt zahlreiche Anbieter kostenloser und kostenpflichtiger Passwort-Manager für PC und Smartphone.
- Auch sollen Passwörter keinesfalls per SMS, E-Mail oder als E-Mail-Anhang versendet werden.
- Wenn möglich sollte eine Zwei-Faktor-Authentisierung genutzt werden.

Schutz vor Tracking

Durch verschiedene Techniken versuchen Anbieter, Nutzerprofile zu erstellen. Davor kann man sich nur bedingt schützen. Folgende Maßnahmen können das Tracken der eigenen Daten vermindern.

- **Optimieren der Browsereinstellungen**
- Nicht Google als Startseite festlegen. Verwenden Sie Alternativen zur Suche (z.B. DuckDuckGo)
- PopUps im Browser sperren
- Cookies von Drittanbietern blocken
- Chronik beim Schließen des Browsers löschen
- Deaktivieren des Speicherns von Formulardaten und Sucheingaben
- Aktivieren der „Do not Track“-Option

- **Installation von „Anti-Schnüffel-Extensions“ und Adblockern**
  Beispiele:

- Avast Online Security:
  Warnt vor dem Besuch von verdächtigen Seiten. Bewertet jedes Suchergebnis vor Aufruf.

- uBlock Origin:
  Blockt Werbung aller Art, Social Media Buttons, Tracker, Malware und vieles mehr (Optionen sichten).

- Google Analytics Opt Out:
  Weist die Google Analytics an, keine Daten zu erheben. Zu finden unter den Namen „No Google Analytics“ oder „Deaktivierungs-Add-on von Google Analytics“.

- Privacy Badger:
  Lernt automatisch, unsichtbare Tracker zu blockieren. Anstatt Listen darüber zu führen, was blockiert werden soll, erkennt Privacy Badger Tracker automatisch anhand ihres Verhaltens.

- HTTPS Everywhere:
  Prüft bei jedem Seitenaufruf über http, ob die Seite nicht auch in https verfügbar ist, und schaltet auf diese sichere Verbindung um.

Vorsicht bei der Nutzung kostenloser Dienste

Die Nutzung kostenloser Dienste wird in der Regel mit Erhebung und Weiterverwendung Ihrer privaten Daten bezahlt.

- Bilderpools
  In fast allen AGB‘s wird die Aufgabe der eigenen Rechte an den Bildern festgelegt. Die Anbieter dürfen ihre Bilder weiterverwenden und weiterverkaufen.

- Suche
  Kaum ein Dienst gibt mehr Auskunft über das Surf- und Nutzungsverhalten als eine Suchmaschine, wenn alle Suchen im Web über diese eine Maschine laufen. Nicht nur die Suche, auch, was angeklickt wird, wird erfasst.

- Terminabstimmungen (z.B.doodle.de)
  Nicht nur, mit wem ich mich verabreden möchte, auch, wo diese Menschen sitzen, welche IT-Ausstattung sie haben, wie sie heißen usw. läuft an einer Stelle zusammen. Eine datenschutzkonforme Alternative ist z.B. der DFN Terminplaner (terminplaner.dfn.de).

Freie WLAN's
Vorsicht bei der Nutzung freier WLAN's, oft stecken Absichten dahinter. Beispielsweise in Einkaufszentren werden die für Kunden angebotenen WLAN's verwendet, um die Kunden zu tracken und Bewegungsprofile zu erstellen. Eine weitere Gefahr kann durch die oft unzureichende Sicherheitskonfiguration solcher WLAN's entstehen, aufgrund derer sich die einzelnen Teilnehmer gegenseitig sehen können. Dritte könnten also unberechtigte Zugriffsversuche auf das eigene Gerät durchführen.
Um öffentliche WLAN-Hotspots sicher nutzen zu können, empfiehlt sich die Nutzung eines sogenannten VPNs. VPN steht für „virtuelles privates Netzwerk" (auf English Virtual Private Network). Eine VPN-Verbindung stellt eine sichere Verbindung zwischen dem Endgerät und dem Internet her. Auf diese Weise wird der gesamte Datenverkehr über das VPN verschlüsselt. Es schützt außerdem die Online-Identität des Users, indem es die IP-Adresse verbirgt

Videokonferenzsysteme
Bei der Nutzung von Videokonferenzsystemen empfiehlt sich, datenschutzkonforme Systeme zu verwenden, z.B. Senfcall, www.senfcall.de.

Autorenkontakt

Holger Bassarek, Dipl.-Ing. (FH), DLH-Webmaster und DLH-Vorstandsmitglied,
E-Mail: h.bassarek@leukaemie-hilfe.de

Erläuterungen zu Fachbegriffen und Abkürzungen

Adblocker:
Das Wort „Ads" kommt aus dem Englischen und ist eine Abkürzung für „advertisement", zu Deutsch Werbung. Ein Adblocker blockt lästige Werbeanzeigen im Internet ab.

Blog:
Das Blog (auch: der Blog) oder auch Weblog (von World Wide Web und Logbuch) ist ein auf einer Webseite geführtes, meist öffentlich einsehbares Tagebuch oder Journal, in dem eine oder mehrere Personen (Web-Logger, kurz Blogger) Aufzeichnungen führen, Sachverhalte protokollieren oder Erfahrungsberichte und Gedanken niederschreiben.

Bookmarks/ Favoriten:
Lesezeichen, die man benutzt, um Angebote im Internet wiederzufinden.

Botnetze:
Ein Netzwerk von Computern, die mit Schadsoftware infiziert sind und von Kriminellen über das Internet zusammengeschaltet und kontrolliert werden. Die Botnetze werden dann z.B. zum massenhaften Versenden von Spam- oder Phishing-Mails oder für Angriffe auf Webseiten (DDoS Angriffe: Distributed Denial of Service) genutzt.

Browser/ Webbrowser:
Mit dem Browser werden die WWW-Seiten abgerufen und auf dem PC dargestellt. Bekannte Browser sind z.B. Microsoft Edge, Mozilla Firefox, Google Chrome, Apple Safari. Die Browser können über Plugins/Extensions z.B. Adblocker im Funktionsumfang erweitert werden.

Cache:
Lokales Verzeichnis, in dem der Web-Browser die heruntergeladenen Daten zwischenspeichert, um sich ggf. ein erneutes Laden vom Server zu sparen.

Cookies:
Informationen, die der Web-Server an den Browser sendet, beispielsweise eine Kundennummer, über die der Benutzer bei einem Folgebesuch identifiziert werden kann.

Domain:
Domains (siehe auch „Internet-Adresse") sind eine Adressierungsmethode, um Computer im Internet (auch Hosts/Server genannt) zu identifizieren und zu lokalisieren. Die Rechner untereinander erkennen sich über rein numerische Bezeichnungen, sog. IP-Adressen. Menschen können sich Begriffe und Bezeichnungen aber meist leichter merken als Zahlenkolonnen. Daher wurde das Domain Name System (DNS) entwickelt, das es erlaubt - innerhalb gewisser Regeln - frei wählbare Wörter, Namen und Begriffe statt Ziffern zu verwenden. Die Hosts können damit vom Internetnutzer sowohl über die IP-Adresse als auch über die Eingabe der Domain erreicht werden. Daneben lassen sich über das DNS weitere Dienste und Informationen abrufen. Wenn eine Domain im Internet aufgerufen wird, übernehmen spezielle Rechner, sogenannte Nameserver, die Aufgabe, eine „Übersetzung" in die IP-Adresse vorzunehmen. Wegen der Eindeutigkeit darf jede Domain, wie auch eine IP-Adresse, weltweit jeweils nur einmal registriert werden.

Download:
Übertragen (Herunterladen) von Daten von einem fremden auf den eigenen Rechner.

E-Mail:
Electronic Mail oder kurz E-Mail (email, eMail) ist der Austausch von Nachrichten über das Internet. E-Mail hat mehrere Vorteile. Die E-Mails erscheinen direkt auf dem PC (Personal Computer) und können auch wiederum direkt beantwortet wer-

den. E-Mails werden bis zum Abruf durch den Benutzer auf einem E-Mail-Server zwischengespeichert, auch wenn der PC nicht online ist. E-Mails können sehr einfach erstellt und versendet werden. Eingehende E-Mails können weiterversendet oder strukturiert abgelegt werden. Dateien oder Bilder können an eine E-Mail angehängt werden.

Extensions:
Auch Softwareerweiterung oder Plugin. Hier: ein optionales Software-Modul, das die Funktion des Internetbrowsers erweitert oder verändert.

FAQ:
Frequently Asked Questions; häufig gestellte Fragen mit Antworten.

Homepage:
Startseite (erste Seite) eines Web-Seiten-Angebots.

HTML / Hyper Text Markup Language:
HTML ist eine einfache Seitenbeschreibungssprache für die Erzeugung von WWW-Seiten. In ihr sind Befehle für die Schriftdarstellung, Grafikeinbindung, Formularelemente, das Seitenlayout und die Verknüpfung (Link) von WWW-Seiten definiert.

HTTP:
Ein in Netzwerken verwendetes Protokoll (Hypertext Transfer Protocol; "Hypertext-Übertragungsprotokoll") zur Datenübertragung. Es wird hauptsächlich eingesetzt, um Webseiten aus dem WWW in einen Browser zu laden

HTTPS:
Ein in Netzwerken verwendetes Protokoll (Hypertext Transfer Protocol Secure; „sicheres Hypertext-Übertragungsprotokoll“), um im WWW Daten sicher verschlüsselt zu übertragen

Internetadresse:
Die Internetadresse besteht aus dem verwendeten Protokoll, dem Internetdienst, dem Domainnamen und der Domainnamenendung (Top-Level-Domain):
z. B. http://www.firma.de
„http“ ist das verwendete Protokoll (**H**yper**t**ext**T**ransfer**P**rotokoll), *„www“* steht für WorldWideWeb, *„firma“* steht für den gewählten Namen
„.de“ ist die Domainnamenendung („de“ für Deutschland).

Internetadressen-Endungen / Top-Level- Domain:
Top-Level-Domains (TLDs) sind Teil der Internetadresse und werden unterschieden in allgemeine (z.B. .com, .net, .org) und länderspezifische TLDs (z.B. .de, .at, .ch).

Link:
Verweis oder Verknüpfung in HTML-Seiten zu anderen Seiten. Sie werden im Browser meist farblich und unterstrichen hervorgehoben.

Malware:
Auch Schadprogramm, Evilware oder Junkware. Computerprogramme, die unerwünschte oder auch schädliche Funktionen ausführen.

Nameserver:
Auch Domain Name Server (DNS) genannt; Rechner im Internet, der eine Tabelle mit Domainnamen und den zugehörigen IP-Adressen enthält

Passwort-Manager:
Passwort-Manager sind Programme, die Benutzernamen und Passwörter verwalten. Mittels Verschlüsselung und eines komplexen Masterpassworts verwahren Passwort-Manager die Passwörter sicher.

Pop-Up:
Hier: ein Browserfenster, das sich zusätzlich und im Vordergrund der eigentlichen Browseroberfläche öffnet.

Server:
Ein Server ist ein Programm, welches auf die Kontaktaufnahme eines Client-Programmes (Programm auf dem Computer des Nutzers) wartet und nach Kontaktaufnahme mit diesem Nachrichten austauscht. Auch der Rechner, auf dem die Server-Software läuft, wird als „Server“ bezeichnet. Auf einem Server können Daten und Dokumente gespeichert werden, die von dem Client-Programm, wie z.B. dem Webbrowser Ihres Computers, abgerufen werden können.

Social Engineering:
Unter Social Engineering versteht man das Ausspionieren des persönlichen Umfeldes eines Opfers, um geheime Informationen zu erlangen. Gerade die allseits beliebten „Sicherheitsfragen“ in Unternehmen mit dilettantischen IT-Sicherheitskenntnissen sind der optimale Angriffspunkt für Social Engineering. Denn, wie der erste Arbeitgeber oder die Oma mit Vornamen heißt oder wann die Katze Geburtstag hat, lässt sich für geübte Social Engineers leicht und schnell herausfinden. Daher sollten Sie, sofern man Sie zur Erfassung solcher „Sicherheitsantworten“ nötigt, immer FALSCHE Antworten eingeben und sich diese an einem sicheren Ort vermerken.

Skript:
Skripte sind kleine Computerprogramme, die auch in E-Mails oder Webseiten eingesetzt werden können. Sie werden oft dazu verwendet, dynamische Seiteninhalte zu erstellen oder Eingaben zu überprüfen.

SMTP:
Simple Mail Transfer Protokoll; Standardprotokoll zum Versand von E-Mails

Spam:
Eine der größten Plagen im Internet sind Spam-E-Mails. Das sind unerwünschte Massen-Mailings, die meist für Produkte werben, die keiner will oder braucht. Oft enthalten Spam-Mails gefährliche Schadsoftware.

Spyware:
Als Spyware (deutsch: Spähprogramm oder Schnüffelsoftware) werden Programme bezeichnet, die Daten eines Computernutzers ohne dessen Wissen oder Zustimmung an Dritte senden.

Ransomware:
Schadprogramme, mit deren Hilfe Eindringlinge Zugriffs- oder Nutzungsverhinderung der Daten eines Computersystems bewirken. Für die Freigabe wird ein "Lösegeld" (engl. "ransom") verlangt.

Tracker/tracken:
Hier: das Nachvollziehen des Benutzerverhaltens des Internetnutzers.

Transfervolumen:
Bewegte Datenmenge, die über eine Leitung – z.B. vom Internet auf den eigenen Rechner – übertragen wird

URL:
Uniform Resource Locator ist die eindeutige Adresse einer einzelnen Internet-Seite oder eines Bildes. Sie besteht aus der Internet-Adresse ergänzt um einen Verzeichnis- und Dateinamen sowie der Endung *.htm oder *.html
z.B. http://www.firma.de/verzeichnis/dateiname.htm

Web-Server:
Mit dem Web-Server (Software) werden Web-Seiten für das Internet verfügbar gemacht (veröffentlicht).

WLAN:
Wireless Local Area Network (deutsch: Drahtloses lokales Netzwerk). Zugang zum Internet über ein lokales Funknetz.

WWW / World Wide Web:
Das WWW ist ein leistungsfähiges, Hypertext-orientiertes Multimediasystem, das über eine grafische Oberfläche gesteuert wird. Dadurch kann der Benutzer ohne weitere Vorkenntnisse verschiedenste Informationen in Schrift, Bild und Ton abrufen. Mit seiner HTML-Sprache (HyperText Markup Language) hat es den großen Vorteil, dass jeder mitgestalten und seine Infos, Neuigkeiten, Bücher, Berichte, Wichtiges und Unterhaltsames im weltweiten Netz präsentieren kann.

Zertifikat:
(SSL-Zertifikat) Hier: ein digitaler Datensatz auf dem Server des Seitenanbieters, der die Online-Kommunikation absichert. Stellt ein Webbrowser eine Verbindung zu einer gesicherten Website her, ermöglicht das SSL-Zertifikat eine gesicherte Verbindung. Das Verfahren ist vergleichbar mit dem Versiegeln eines Briefs vor dem Versenden.

Zwei-Faktor-Authentisierung:
Mittlerweile bieten viele Online-Dienstleister Verfahren an, mit denen die Nutzer oder die Nutzerinnen sich zusätzlich bzw. alternativ zur Passworteingabe identifizieren können. Dies geht z.B. über eine über SMS oder E-Mail versendete Transaktionsnummer oder spezielle Smartphone-APPs.