IKARUS security software

Sicherheitstipps

Wie schütze ich Daten und Geräte?

Computer herunterfahren

Beenden Sie nach der Arbeit alle Programme und schalten Sie den Computer aus. Der Neustart am nächsten Morgen gibt Gelegenheit zum Installieren von Updates, und in der Zeit, in der Ihr Gerät nicht vernetzt ist, kann es auch nicht angegriffen werden.

Auf Veränderungen achten

Manchmal ist ein erfolgreicher Angriff nur minimal wahrnehmbar, z.B. wenn beim Crypto-Mining fremde Rechnerkapazitäten missbraucht werden. Es kommt zu Leistungsabfall, erhöhtem Stromverbrauch, Heißlaufen der Geräte und damit verbunden geringerer Lebensdauer. Eine Verlangsamung der Systeme, vermehrte Werbeanzeigen und ungewohnte Verhaltensweisen können auch auf andere Malware hinweisen. Bitte Geräte und Systeme mit aktueller Antivirensoftware scannen!

Physischen Zugriff beschränken

Verhindern Sie den physischen Zugriff auf Ihre Geräte: Setzen Sie sichere Passwörter und verwenden Sie die Bildschirmsperre, sobald Sie Ihren Rechner unbeaufsichtigt lassen. Auch tragbare Geräte sollten mit Displaysperren geschützt werden - wir empfehlen jedoch, diese Geräte nicht unbeaufsichtigt zu lassen. Achten Sie beim Abrufen oder der Eingabe privater Daten auf neugierige Blicke!

Speichermedien sicher entsorgen

Einfaches Löschen der Inhalte reicht nicht aus, um tatsächlich alle Spuren zu entfernen und die Wiederherstellung der Daten zu verhindern: Besser ist es, Festplatten, USB-Sticks oder CDs physisch zu zerstören oder, falls nicht möglich, mehrfach zu überschreiben.

Vorsicht im WLAN

Kostenlose WiFi-Hotspots können Datenvolumen sparen – jedoch auch Ihre Sicherheit kosten. Freies WLAN ist oft ungeschützt, darüber versendete Passwörter und Daten können relativ einfach von Drittnutzern abgegriffen und missbraucht werden. Auch passwortgeschützte Gäste-Netzwerke sind keine Garantie dafür, dass Ihre Daten nicht von Dritten mitgelesen werden können. Nutzen Sie daher für das Abrufen und Eingeben privater Daten nur gesicherte Verbindungen. Sichern Sie auch zu Hause Ihr WLAN mit einem (selbst gesetzten) Passwort ab.

Sichere Verbindungen nutzen

Achten Sie auf sichere Verbindungen und gültige Zertifikate. Informationen dazu werden in der Adressleiste des Browsers angezeigt. Kontrollieren Sie die korrekte Schreibweise von URLs und Firmennamen: Phishing- Seiten, die Bankdaten oder Passwörter abgreifen wollen, sind oft täuschend echt nachgebildet, falsche URLs oder Domains liefern oft den entscheidenden Hinweis. Folgen Sie daher auch keinen Links zu Seiten, die persönliche Daten verlangen, sondern surfen Sie Dienste wie Ihr Netbanking-Login direkt an.

Makros und JavaScript deaktivieren

Hindern Sie, wenn möglich, JavaScript am automatischen Ausführen oder blocken Sie JavaScript-Inhalte von nicht vertraulichen Quellen. Deaktivieren Sie Makros oder verwenden Sie nur entsprechend signierte Makros. Verlangt ein Dokument, das Ihnen zugesendet wurde, das Aktivieren von Markos, verweigern Sie die Berechtigung im Zweifelsfall.

IKARUS Sales Team | sales@ikarus.at | +43 1 589 95-500
IKARUS Support Team | support@ikarus.at | +43 1 589 95-400

IKARUS
security software

Cookies dankend ablehnen

Kontrollieren und adaptieren Sie gegebenenfalls die Einstellungen Ihrer Browser: Genau wie Suchmaschinen sammeln und speichern sie gerne Daten. Begrenzen Sie diese gespeicherten Daten und löschen Sie Cookies und Cache von Zeit zu Zeit. Wenn möglich lehnen Sie beim Surfen das Setzen von Cookies ab oder beschränken Sie es auf funktionelle Cookies.

Vorsicht bei Downloads

Laden Sie keine „gecrackten“ Programme, Key-Generatoren oder ähnliches aus dem Internet runter: Diese Dienste sind nicht nur illegal, sondern auch beliebte Verstecke für Schadsoftware aller Art. Auch bei legalen Downloads bitte Vorsicht walten lassen und keine Apps aus unbekannten Quellen installieren!

Verknüpfungen vermeiden

Vermeiden Sie das Vernetzen verschiedener Dienste und Accounts und nutzen Sie stattdessen jeweils individuelle Benutzer-Daten. Wurde ein Account geknackt, verhindern Sie damit, dass Angreifer gleich auf mehrere Konten zugreifen – und Sie damit gegebenenfalls völlig aus Ihren eigenen Accounts aussperren – können.

Sicheres Passwort-Management

Verwenden Sie unterschiedliche, komplexe Passwörter für verschiedene Dienste und speichern Sie diese niemals unverschlüsselt auf Ihrem Computer ab. Aktivieren Sie nach Möglichkeit Zwei-Faktor-Authentifizierung (2FA) und benutzen Sie einen Passwortmanager wie KeePass2 oder Lastpass. Passwörter aus Data-Breaches werden in Kombination mit verschiedensten E-Mail-Adressen regelmäßig auch an anderen Diensten ausprobiert, um Accounts zu knacken.

Persönliche Daten schützen

Geben Sie auf vertrauensunwürdigen Seiten niemals persönliche Daten preis. Überlegen Sie gut, was Sie in den sozialen Netzwerken posten: Diese Informationen werden gerne für überzeugend wirkende Phishing-Versuche verwendet. Beachten Sie die Datenschutzbestimmungen von Websites, Legal Notes und Lizenzverein-barungen. Harmlos erscheinende Dienste oder Apps sichern sich womöglich Zugriffs- oder Datenrechte, die weit über die Funktion des beworbenen Dienstes hinausgehen.

Information & Awareness

Behalten Sie die Möglichkeiten und Mittel von Betrugsversuchen (Phishing-Kampagnen, CEO-Fraud, Social Engineering…) im Hinterkopf und informieren Sie sich regelmäßig über aktuelle Bedrohungen und Malware-Kampagnen. Damit lässt sich auch die Neugierde auf „phantastische Videos“ oder die angeblich „letzte Mahnung“ im Attachment, die Betrugsversuchen so oft zum Erfolg verhilft, am sichersten stillen.

Backups anlegen

Aktuelle Gefahren wie Ransomware vedienen sich daran, die Daten ihrer Opfer zu verschlüsseln oder zu blockieren und nur gegen (Bitcoin-) Zahlungen wieder freizugeben. Ein aktuelles Backup aller wichtigen Daten, das vom Computer getrennt aufbewahrt wird und somit nicht verschlüsselt werden kann, macht gegen diese Gefahren unverwundbar. Aber auch bei einem andersartigen Virenbefall hilft ein Backup dabei, das System zu desinfizieren, ohne Daten zu verlieren.

Spezialisten befragen

Bei Unsicherheiten lohnt es sich in jedem Fall, eine/n SpezialistIn zu Rate zu ziehen - sei es die IT-Abteilung des Unternehmens oder der IKARUS Support. Sobald eine E-Mail oder ein Verhalten am PC verdächtig erscheinen, empfehlen wir, die Auffälligkeiten nach Möglichkeit zu dokumentieren und eine professionelle Meinung einzuholen. So können mögliche Angriffe verhindert oder aber bereits erfolgte Infektionen schnell eingedämmt werden, bevor sie sich weiter ausbreiten und größeren Schaden anrichten können.

IKARUS Sales Team | sales@ikarus.at | +43 1 589 95-500
IKARUS Support Team | support@ikarus.at | +43 1 589 95-400