Landkreis Waldshut

IT-Grundschutz Handout

Hinweise zur sicheren Nutzung von IT-Systemen

Inhaltsverzeichnis

1 Grundsätzliches 3

2 Zugang und Zugriff 3

3 Ein gesundes Misstrauen bei Nutzung von E-Mail und Internet 4

4 Virenschutz 4

5 Sichere Passwörter 5

6 Erkennen Sie verdächtige Ereignisse 7

7 Meldung machen 8

8 Links und weitere Information: 8

9 Falls Sie auch Zuhause einen PC oder mobile Geräte benutzen 10

1 Grundsätzliches

Viel Ärger hat sich der erspart, der heikle Dinge gut verwahrt!

Die tägliche Arbeit kann betriebsblind machen. Sie könnten der Annahme erliegen „Bei uns gibt es doch nichts Interessantes…“. Damit liegen Sie sehr wahrscheinlich falsch. Hier ein paar Beispiele, welche Informationen für Außenstehende - auch für nicht berechtigte Interne - sehr verlockend sein könnten:

- ☑ Adressdaten in großer Menge (z.B. KFZ-Halter)
- ☑ Ausgewählte Adressdaten (z.B. Mitarbeiter des Landratsamtes in Führungspositionen, oder alle Besitzer eines Rolls-Royce im Landkreis)
- ☑ Persönliche Daten von Bürgern zu deren Gesundheitszustand oder zur finanziellen Situation
- ☑ Technische Daten und Verfahrensstände (z.B. bei Ausschreibungen)
- ☑ Genehmigungs- und Zulassungsverfahren die z.B. Produktionsanlagen betreffen.
- ☑ Informationen zu Lieferanten und Dienstleistern
- ☑ Besondere Vorkommnisse in Sachen Umweltschutz oder Lebensmittelrecht (Stichwort Gammelfleisch)
- ☑ Notfall- und Katastrophenplanungen (zeigen eventuelle Schwachstellen auf)

2 Zugang und Zugriff

Fremder Zugriff wird erschwert, bleibt der Zugang stets verwehrt!

Zutritts- und Zugangsschutz sind das „A & O“. Verschließen von Büro- und Technikräumen, sperren der IT-Arbeitsplätze auch bei kurzfristiger Abwesenheit durch Aktivieren des Bildschirmschoners mit Passwortschutz und der Kombination. „**WINDOWS-Taste + L**“ oder über „**STRG + ALT + ENTF**“ → Sperren.

Falls ein Angreifer uneingeschränkten physischen Zugriff auf Ihren Computer bekommt, ist das nicht mehr Ihr Computer.

Technische Sicherheit durch Hard- und Software. Darum kümmert sich Ihre IT-Abteilung.

3 Ein gesundes Misstrauen bei Nutzung von E-Mail und Internet

Verzichte auf den Mailversand, ist der Inhalt sehr pikant!

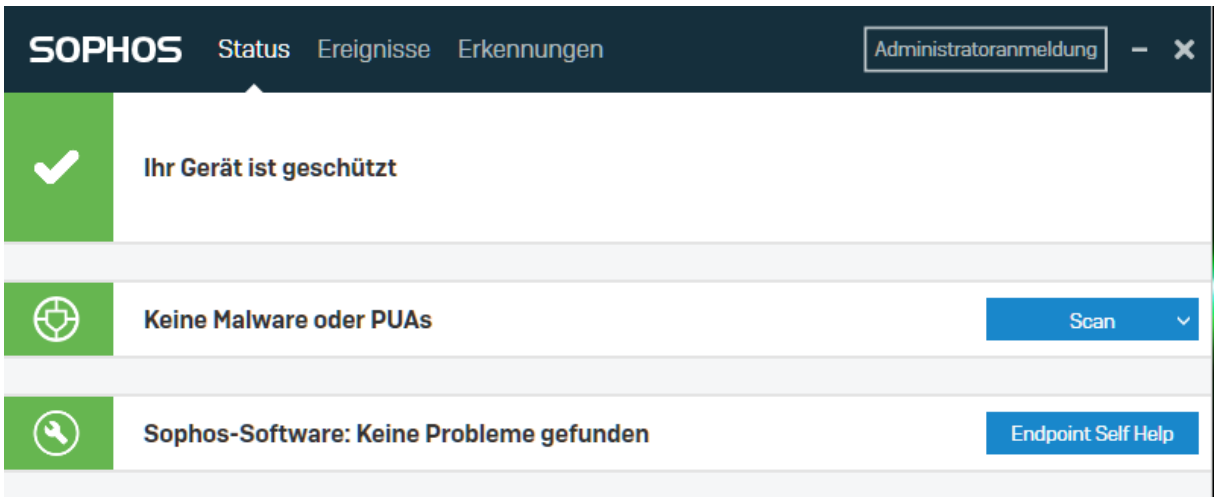
- ☑ Keine personenbezogenen Daten über E-Mail verschicken, auch nicht innerhalb des Landratsamtes. Verwenden Sie vertrauliche Kommunikationswege wie z.B. Cryptshare.
- ☑ Das elektronische Postfach nach Vorgaben regeln (Vertretung, Postfachspeichergröße, Abwesenheitsassistent)
- ☑ Ordnung halten im E-Mail-Postfach
- ☑ Das E-Mail-Postfach ist keine Archivierung
- ☑ E-Mails werden behandelt wie normale Post und müssen in die Akte abgelegt werden
- ☑ Die Sicherung der E-Mails/der Postfächer wird zentral durchgeführt
- ☑ Keine Umleitung dienstlicher E-Mails an private Postfächer

Regelungen: Dienstanweisung und Dienstvereinbarung Internet
Dienstanweisung IT

4 Virenschutz

Jede Art von Schad-Software muss unbedingt vermieden werden. Hierzu betreibt die Abteilung IT ein mehrstufiges System, sowie einen sog. SPAM-Filter. Als SPAM werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, die dem Empfänger unverlangt zugestellt werden und häufig werbenden Inhalt oder Schadsoftware enthalten.

Aktuell kommt im Landratsamt Schutzsoftware des Herstellers Sophos ein. Sollten Sie eine Benachrichtigung von Sophos erhalten, setzen Sie sich umgehend mit der IT-Hotline in Verbindung. Zusätzlich werden Ereignisse auch zentral durch die IT überwacht. Zur Kontrolle oder zum Auslösen manueller Scans können Sie Sophos auch über das Symbol  im Windows-Infobereich aufrufen.



Wie sich der SPAM-Filter meldet, sehen Sie hier

LRAWT-Spamfilter: Sammelbenachrichtigung

LRAWT Postmaster

Gesendet: Mi 30.10.2013 19:00

An: Köhler, Anita

iQ.Suite Sammelbenachrichtigung

Sammelbenachrichtigung für Quarantäne 'Anti-Spam: Mittel' Server 'F1WALSE02' (F1WALSE02.lrw01.intra)

Aktuell erstellt am:	2013-10-30, 19:00:00.
Zuletzt erstellt am:	2013-10-30, 18:00:00.
Zusammenfassung für:	Anita.Koehler@landkreis-waldshut.de
Zwischenbericht anfordern:	Zwischenbericht anfordern (HTTP)

HTTP	Zustelldatum und -zeit	Absender	Betreff
Anfordern (HTTP)	2013-10-30T18:35:58	newsletter@esri.com	Call for Papers Ends November 1

5 Sichere Passwörter

Die Sicherung ist null und nichtig, nimmt man das Passwort nicht so wichtig!

Hier ein paar Tipps für Methoden, wie man sich ein schweres Passwort ausdenkt:

<u>Mit System</u>

☑ Verwenden Sie ein System, aber sagen Sie es niemanden. Aber Achtung: jede Systematik birgt die Gefahr, dass jemand eine Variante erraten kann. Behalten Sie darum Ihre Art der Passwort-Bildung unbedingt für sich. Geben Sie auch aus diesem Grund niemals eines Ihrer Passwörter weiter.

- ☑ Passwörter regelmäßig ändern: Jedes Passwort sollte in regelmäßigen Zeitabständen geändert werden. Viele Programme erinnern automatisch daran, wenn das Passwort schon ein halbes Jahr benutzt wird.
- ☑ Passwörter nicht aufschreiben: Auch, wenn es bei selten genutzten Zugangsdaten schwerfällt: Grundsätzlich sollten Nutzer sich Passwörter nicht notieren.
- ☑ Unterschiedliche Passwörter verwenden: Problematisch ist die Gewohnheit, einheitliche Passwörter für viele verschiedene Zwecke zu verwenden. Denn gerät das Passwort einer einzelnen Anwendung in falsche Hände, sind auch die anderen Anwendungen nicht mehr geschützt.
- ☑ Voreingestellte Passwörter ändern: Bei vielen Softwareprodukten werden bei der Installation (beziehungsweise im Auslieferungszustand) in den Accounts leere Passwörter oder allgemein bekannte Passwörter verwendet. Diese sollten vom Nutzer schnellstmöglich geändert werden.

Schlechte Passwörter sicher machen

Beispiel: das schlechte Passwort „Test“

- ☑ Anhängen 16.01.89 -> „test160189“
- ☑ Noch besser „16test0189“ mit Sonderzeichen-> „(16test0189)“

Gute Auswahl

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt auf seiner Webseite www.bsi-fuer-buerger.de Tipps, wie Nutzer ihre Passwörter sicherer machen können.

- ☑ Ein komplexes Passwort wählen
- ☑ Mindestens acht Zeichen lang sein, noch besser 12 Zeichen
- ☑ nicht im Wörterbuch stehen
- ☑ Neben Buchstaben sollte es auch Ziffern und Sonderzeichen enthalten

Tabus

- ☑ Keine Namen verwenden, auch den eigenen nicht
- ☑ Keine Namen von Familienmitgliedern
- ☑ Keine Namen des Haustieres
- ☑ Keine Namen der besten Freunde
- ☑ Keine Namen der Lieblingsstars
- ☑ Passwörter nicht aufschreiben

Kreativ werden

- ☑ Um ein komplexes und dennoch leicht zu merkendes Passwort zu konstruieren, empfiehlt sich ein Merksatz als Eselsbrücke. Dabei denkt sich der Nutzer einen Satz aus und benutzt von jedem Wort beispielsweise nur den ersten Buchstaben. Anschließend verwandelt man bestimmte Buchstaben in Zahlen oder Sonderzeichen. So wird zum Beispiel aus dem Merksatz "Morgens stehe ich auf und putze meine Zähne." das Passwort "Ms1a&pmZ" für „Morgens stehe ich auf und putze meine Zähne“.

- ☑ Oder: Oder „WdhkbvnaM!“ -> können Sie sich nicht merken? Lösung: Was du heute kannst besorgen verschiebe nicht auf Morgen! Achtung Sie durchaus auch auf die Groß/Kleinschreibung.
- ☑ So könnten sie beispielsweise alle „a“ in Namen durch die Zahl „1“ ersetzen, aus dem Passwort „Andrea“ würde „1ndre1“.
- ☑ Oder ersetzen Sie alle „i“ durch ein „!“ Willi wird also zu „W!ll!“
- ☑ Oder Sie fügen die Telefonnummer ein, nach jedem Buchstaben eine Ziffer, so würde aus „Willi“ und „876530“ das Passwort „W8i7l6l5i3“.
- ☑ Falls Sie Ihr Passwort oft ändern, verwenden Sie eine Serie; „omo-1ndre1“, „persil-1ndre1“, „ariel-1ndre1“.

Unterschiedliche Passwörter für verschiedene Konten verwenden
Für verschiedene Dienste im Internet (eBay, Amazon, PayPal etc.) sollten Sie unterschiedliche Benutzernamen und Passwörter verwenden. Eine gute Idee ist, den jeweiligen Firmennamen mind. teilweise im Benutzernamen und im Passwort zu nennen und dabei ein ausreichend langes Kennwort zu benutzen. Wenn die Passwörter und Benutzernamen in Internetlisten auftauchen, kann das betroffene Portal identifiziert werden.

Die genauen Richtlinien und Informationen für die sichere Anwendung von Passwörtern im Landratsamt Waldshut finden Sie im Intranet unter der DA-IT, Anlage 2.

6 Erkennen Sie verdächtige Ereignisse

Eine unbekannte Person in einem nicht öffentlichen Bereich könnte schlechte Absichten haben. Sie werden mit folgenden Situationen konfrontiert:
- Ein Anrufer weigert sich eine Rückrufnummer anzugeben.
- Der Anfrager spielt stark seine Autorität aus.
- Es wird massiv auf eine hohe Dringlichkeit hingewiesen.
- Eine Drohung mit negativen Konsequenzen bei Kooperationsverweigerung.
- Ihre Rückfragen werden als lästig abgetan.
- Es werden auffallend Namen von wichtigen und bekannten Personen fallen gelassen.
- Auch Komplimente und Schmeicheleien sollten Sie wachsam werden lassen.

Es handelt sich hier um Indizien und Anzeichen, von denen jedes einzelne auch völlig harmlos sein kann. In der Summe und in Bezug auf das Anliegen könnte ein gewisses Misstrauen angemessen sein. Die angeführten Warnzeichen sind symptomatisch für einen Angriff auf Ihre Daten durch einen nicht-technischen Hacker (Social Engineer, Trickbetrüger).

Ihre Reaktion bei einem Verdacht
Stellen Sie fest, ob die Person wirklich die ist, für die sie sich ausgibt. Fragen Sie sich: Ist die Person berechtigt, die angefragte Information zu bekommen? Erteilen Sie angemessen sparsam Auskunft.

- ☑ Vermeiden Sie Unsicherheit, falls der Anrufer Sie unter Druck setzen möchte.
- ☑ Stellen Sie fest, woher ein Anruf kommt.
- ☑ Rufen Sie die Person selbst per Festnetz zurück.
- ☑ Lassen Sie sich einen Bürgen nennen, der die Identität des Anfragers bestätigen kann.
- ☑ Ein nur internen Personen bekanntes „geteiltes Geheimnis“ kann abgefragt werden.
- ☑ Anruf bei den direkten Vorgesetzen des Anfragers, um das Anliegen zu prüfen
- ☑ Halten Sie sich an die rechtlichen Vorgaben.
- ☑ Beachten Sie die Grundlagen des Datenschutzes.
- ☑ Initiieren Sie nicht die Installation unlizenzierter Software.
- ☑ Beachten Sie das Urheberrecht (z. B. bezüglich der Nutzung von Material aus dem Internet).
- ☑ Fragen Sie im Zweifelsfall Ihren Vorgesetzten.
- ☑ Melden Sie Ihren Verdacht auf einen Sicherheitsvorfall zeitnah.

7 Meldung machen

Rennt der Admin in den Keller, war der Hacker wieder schneller.

Falls Ihnen etwas „spanisch“ vorkommt und Sie den Verdacht hegen, dass jemand mit den Mitteln des „Social Engineering“ versucht, an Information zu kommen, melden Sie das bitte zeitnah an Ihre Vorgesetzten und Ihre IT-Abteilung. Merken Sie sich bitte Datum, Uhrzeit und Inhalt Ihres Kontaktes. Auch Kleinigkeiten könnten wichtig sein. Bei Vorfällen und Verdacht melden Sie sich bitte hier:

Abteilung IT
Telefon **07751/86-1111**
E-Mail **Hotline@Landkreis-Waldshut.de**

Störungen im Bereich Telefonie
E-Mail **Telefon@Landkreis-Waldshut.de**

Datenschutzverstöße
Frau Christina Mutter
Telefon **07751/86-7200**
E-Mail **Datenschutz@Landkreis-Waldshut.de**

8 Links und weitere Information:

IT Technik Seite	http://www.heise.de/security
Bundesamt für Sicherheit in der Informationstechnik	*BSIFB - Startseite BSI für Bürger*

Der Bundesdaten-schutzbeauftragte	http://www.bfdi.bund.de
Datenschutzgrund-verordnung	https://www.datenschutz-grundverordnung.eu/
Schutz von Kindern und Jugendlichen	https://www.klicksafe.de/

Weitere Informationen, Vorschriften und Regelungen finden Sie im Intranet: http://intranet.landkreis-waldshut.net/423705.html

9 Falls Sie auch Zuhause einen PC oder mobile Geräte benutzen

Für alle, die sich über die Gefahren im Internet informieren möchten, hält das BSI das Informationsportal BSI für Bürger bereit. Hier werden auch für Technik-Laien verständlich die Risiken der digitalen Welt erklärt und Tipps zum Schutz gegen die wachsenden Internet-Gefahren gegeben. Die Inhalte reichen vom Online-Banking und Internet-Shopping bis zum Phishing, WLAN und der Internettelefonie. Auch werden kostenlose Schutzprogramme empfohlen.

<u>10 Tipps für das sichere Surfen:</u>

1. Installieren Sie ein *Virenschutzprogramm* und ein *Anti-Spyware-Programm* und halten Sie diese immer auf dem aktuellen Stand.
2. Setzen Sie eine *Personal Firewall* ein und aktualisieren Sie diese regelmäßig. Sie schützt bei richtiger Konfiguration vor Angriffen aus dem Internet und verhindert bei einer Infektion des PCs mit einem Computerschädling, dass ausspionierte Daten an einen Angreifer übersendet werden können.
3. Achten Sie darauf, ob neue *Sicherheitsupdates* für Ihr Betriebssystem und sonstige von Ihnen installierte Software vorliegen und führen Sie diese durch.
4. Arbeiten Sie nach Möglichkeit nicht als Administrator an Ihrem PC. Denn so können Schadprogramme noch mehr Unheil anrichten. Richten Sie für alle Nutzer eines PCs *unterschiedliche Benutzerkonten* ein. Vergeben Sie für diese Konten nur die Berechtigungen, die der jeweilige Nutzer für seine Arbeit braucht. So werden auch private Dateien vor dem Zugriff Unberechtigter geschützt. Manche Computerzeitschriften vertreten die Meinung, dass bei Windows 10/11 diese Vorgehensweise nicht mehr nötig wäre. Wir empfehlen weiterhin eine Trennung.
5. Gehen Sie sorgfältig mit Ihren *Zugangsdaten* um: Halten Sie Kennwörter und Benutzernamen sowie Zugangscodes für Dienste (z. B. beim Online-Banking) unter Verschluss. Wechseln Sie Passwörter in regelmäßigen Abständen.
6. Seien Sie vorsichtig beim *Öffnen von E-Mail-Anhängen*. Schadprogramme werden oft über Dateianhänge in E-Mails verbreitet. Im Zweifelsfall fragen Sie vorsichtshalber beim Absender nach, ob der Dateianhang tatsächlich von ihm stammt.
7. Seien Sie vorsichtig bei *Downloads von Web-Seiten*. Vergewissern Sie sich vor dem Download von Programmen aus dem Internet, ob die Quelle vertrauenswürdig ist und bringen Sie vor dem Download Ihr Virenschutzprogramm auf den aktuellsten Stand.
8. Seien Sie zurückhaltend mit der *Weitergabe persönlicher Informationen*. Online-Betrüger steigern ihren Erfolg, indem sie individuell auf ihre Opfer zugehen: Zuvor ausspionierte Daten, wie etwa Surf-Gewohnheiten oder Namen aus dem persönlichen Umfeld, werden genutzt, um Vertrauen zu erwecken.

9. Wenn Sie Übertragungstechnologien wie Voice over IP (VoIP) oder Wireless LAN (WLAN) einsetzen, achten Sie besonders auf die *Verschlüsselung Ihrer Kommunikation*, damit die Übertragung Ihrer Daten nicht von Dritten mitgelesen bzw. Gespräche nicht abgehört werden können.
10. Kommt es trotz aller Schutzmaßnahmen zu einer Infektion des PCs mit einem Schädling, können wichtige Daten verloren gehen. Um den Schaden möglichst gering zu halten, sollten Sie regelmäßig *Sicherungskopien Ihrer Dateien* auf externen Medien erstellen.

Zusammenfassung

Online-Banking ist ein lohnenswertes Ziel für Angreifer. Vorfälle dieser Art kommen regelmäßig vor. Für die Sicherheit Ihrer privaten Infrastruktur sind Sie verantwortlich.

Immer wieder kommt es vor, dass E-Mails mit gefälschten Anhängen mit Schadsoftware von vermeintlich seriösen Absendern verschickt werden. Hier gilt es, Besonnenheit und ein gesundes Misstrauen zu zeigen.

- ☑ Die Bank ruft nicht an, sie schickt keine E-Mails
- ☑ Keine Kontoinformationen weitergeben
- ☑ Wenn Sie eine solche E-Mail erhalten haben: nichts anklicken, nichts öffnen, nichts eintippen
- ☑ Notfalls bei der Bank anrufen
- ☑ Wenn möglich kein Online-Banking über Tablet oder Smartphone

Vorsorge treffen für Ihre Technik

- ☑ Einsatz aktueller Virenscanner
- ☑ Firewall Software aktivieren
- ☑ Aktuelle Programme einsetzen, Updates installieren
- ☑ Aktuelles Betriebssystem mit allen Updates
- ☑ WLAN nur über den Netzwerkschlüssel (MACs)
- ☑ Nicht mit Administratorrechten in das Internet
- ☑ Keine Software aus unbekannten Quellen installieren
- ☑ Nur populäre Apps von offiziellen Plattformen nutzen

Literaturempfehlung

Rudi Klausnitzer: „Das Ende des Zufalls“

Stand: Februar 2025