Was bringt die Systeme zum Stillstand?
Eine Studie identifiziert mehrere Hauptursachen für Ausfallzeiten:

Menschliches Versagen: Der Spitzenreiter unter den Ursachen. Ein kleiner Fehler kann Stunden der Behebung nach sich ziehen. Unter diesem Punkt subsummieren sich die beiden weiteren Hauptursachen von Ausfallzeiten: Sicherheitsvorfälle und Anwendungs- bzw. Infrastrukturprobleme.
Cyberangriffe: 56 % der Ausfallzeiten sind auf Sicherheitsvorfälle wie Phishing-Angriffe zurückzuführen.
Anwendungs- bzw. Infrastrukturprobleme: 44 % der Ausfallzeiten sind auf Anwendungs- oder Infrastrukturprobleme wie Softwarefehler zurückzuführen.

11 Goldene Regeln zur Erhöhung von IT-Sicherheit & Datenschutz

Bitte halten Sie folgende Regeln ein um Schaden von sich und anderen abzuwenden.
Es ist erwiesen, dass ein Großteil erfolgreicher Angriffe möglich war, weil die Rechner schlecht konfiguriert waren. Die hier beschriebenen Maßnahmen schaffen eine ausreichende Grundsicherheit gegen aktuelle Bedrohungen und sollten von allen Nutzern umgesetzt werden.

1. Betriebssystem aktuell halten

Halten Sie Ihr Betriebssystem stets aktuell, indem Sie verfügbare Updates zeitnah einspielen, da bekannte Schwachstellen für automatisierte Angriffe gegen verwundbare Systeme ausgenutzt werden.

Unser Angebot: Regelmäßige Wartungen, mindestens alle 12 Monate für jedes IT-System.

2. Virenscanner einsetzen und aktuell halten

Schützen Sie Ihren Rechner vor der Infizierung mit Schadsoftware wie Viren, Würmern und Trojanischen Pferden durch die Nutzung eines Virenscanners. Die bloße Installation einer derartigen Software ist allerdings für einen wirksamen Schutz nicht ausreichend. Entscheidend sind die Aktualität und die richtige Konfiguration der wichtigsten Funktionen des Programms.

Unserer Voraussetzung: WEBROOT Virenschutz flächendeckend auf allen Systemen, in Kombination mit Microsoft Defender.

3. Anwendungsprogramme richtig konfigurieren und aktuell halten

Hierzu gehören insbesondere Office-Programme (MS-Office, OpenOffice, Acrobat, …), Internetbrowser und E-Mail-Programme, aber auch Programme zum Chatten oder zum Abspielen von Multimediainhalten (Windows Mediaplayer, Realplayer, Winamp, …). Durch gezielt manipulierte Webseiten und Dateien ist das Bedrohungspotential hier mittlerweile genauso hoch wie bei Serverdiensten, die Anwendungen werden aber im Gegensatz zu diesen bei einem Betriebssystemupdate nicht mit aktualisiert.

4. Sichere Passwörter verwenden

Alle Benutzerkonten eines Systems müssen mit einem Passwort versehen sein, da der Rechner sonst leicht über das Netzwerk angreifbar ist. Insbesondere wird bei vielen Standardinstallationen von Windows kein Administratorkennwort gesetzt! Passwörter sollten einige Mindestanforderungen bezüglich Länge und Komplexität erfüllen, damit sie nicht durch einfaches (evtl. automatisiertes) Durchprobieren erraten werden können.
Passwort Generator ツ - Sicheres Passwort bei datenschutz.org

Unser Angebot: Eine Passwortliste in Excel mit Passwortschutz, einfach aber effektiv!

5. Nicht mit Administratorrechten arbeiten

Sie sollten im Normalfall lokal nicht mit Administratorrechten arbeiten, sondern lediglich mit den eingeschränkten Rechten eines normalen Benutzers. Bei allen modernen Betriebssystemen können Benutzerkonten mit verschiedenen Rechten versehen werden. Einen unbegrenzten Zugriff auf alle Funktionen des Betriebssystems erhalten Benutzerkonten der Kategorie "Administrator" bzw. "root". Bei Konten der Kategorie "Benutzer" bzw. "eingeschränkt" sind die Rechte dagegen limitiert.

Administratorrechte sind notwendig, um Konfigurationen vorzunehmen oder zu ändern. Die Arbeit mit Administratorrechten ermöglicht es vielen Schadprogramme erst ihre schädigende Wirkung voll entfalten zu können. Ein erfolgreicher Angreifer verfügt so automatisch ebenfalls über Administratorrechte.

Nicht benötigte Benutzerkonten sollten deaktiviert oder gelöscht werden.

Falls Sie unter Windows mit eingeschränkten Rechten arbeiten, können Sie einzelne Anwendungen mit Administratorrechten laufen lassen, indem Sie im Programm-Menü oder im Explorer das entsprechende Programm mit der rechten Maustaste anwählen und den Menüpunkt „Ausführen als..“ anwählen.

Praktische Umsetzung: Anlage von einem Admin-Benutzer lokal oder in der Domäne „**pcAdmin“**

6. Software und Daten aus sicheren Quellen nutzen

Software aus nicht vertrauenswürdigen Quellen (z.B. P2P-Tauschbörsen oder inoffizielle Webseiten) enthält häufig Schadsoftware wie Viren, Würmer, Trojaner und Rootkits. Beim Öffnen bzw. Ausführen der entsprechenden Datei(en) wird die Schadsoftware aktiv, vielfach ohne dass der Nutzer dieses bemerkt. Dabei ist es unerheblich, ob es sich um eine manipulierte Anwendung oder um manipulierte Daten für eine verwundbare Anwendung handelt.

Nutzen Sie deshalb ausschließlich Originalsoftware/-daten und beziehen Sie diese möglichst direkt vom Hersteller bzw. von einer vertrauenswürdigen Quelle.

Installieren Sie nur wirklich benötigte Software.

Unser Angebot: Unterstützung per Fernwartung.

7. Rechner vor unberechtigtem Zugriff schützen

Lassen Sie Ihren Rechner nicht unbeobachtet, wenn Sie angemeldet sind. Loggen Sie sich aus, sperren Sie den Zugriff oder aktivieren Sie einen Bildschirmschoner mit sicherem Passwort, wenn Sie Ihren Arbeitsplatz verlassen, auch wenn es sich nur um eine vermeintlich kurze Zeitspanne handelt.

Schalten Sie Ihren Rechner aus, wenn Sie Ihren Arbeitsplatz für längere Zeit verlassen, wie zum Beispiel zum Feierabend.

Unsere Empfehlung: Bildschirmschoner nach 5-10 Min. aktivieren oder einfach (Windows + L) drücken

8. Keine zweifelhaften E-Mails bearbeiten oder beantworten

Führen Sie grundsätzlich keine Software aus, die Ihnen als E-Mail-Anhang zugesandt wird. Deaktivieren Sie im E-Mail-Programm die automatische Anzeige bzw. das Ausführen von E-Mail-Anhängen. Misstrauen Sie E-Mails, die die Aufforderung enthalten, Software zu installieren oder Passwörter, Kreditkartennummern, PINs, TANs oder ähnliches zu übermitteln. Antworten Sie nicht auf E-Mails mit unerwünschtem oder zweifelhaftem Inhalt, auch nicht, um die Versendung dieser E-Mails abzubestellen. Virenbefallene E-Mails täuschen in der Regel vertraute Absenderadressen vor. Misstrauen Sie unerwarteten E-Mails und insbesondere ihren Dateianhängen. Deaktivieren Sie nach Möglichkeit die HTML-Ansicht von E-Mails und nutzen Sie stattdessen die Textansicht. Prüfen sie alle auf den Rechner geladenen Dateien mit einem Virenscanner.

9. Sensible Informationen nicht leichtfertig preisgeben

Seien Sie misstrauisch, wenn Sie jemand wegen eines (vermeintlichen) Problems kontaktiert, und von Ihnen sensible Daten wie Passwörter oder Konfigurationseinstellungen wissen möchte. Externe Dienstanbieter werden Sie nicht nach Ihrem Passwort fragen.

Lassen Sie sich im Zweifelsfall den Namen des IT-Verantwortlichen nennen und rufen Sie Ihn unter der Telefonnummer zurück.

10. Nichtbenötigte Dienste deaktivieren

Entfernen Sie nicht benötigte Dienste und Anwendungsprogramme oder installieren Sie diese erst gar nicht. Falls Dienste/Programme nicht permanent benötigt werden (Chat-Client, …), dann sollten diese manuell gestartet und nach Gebrauch wieder deaktiviert/beendet werden.

11. Daten/System sichern

Die sorgfältige Anwendung der Goldenen Regeln verbessert die Sicherheit Ihres Systems und der darauf gespeicherten Daten. Ein absolut sicherer Schutz gegen Angriffe, Anwenderfehler oder Hardwareschäden ist leider nicht möglich. Da Dateien im Schadensfall auch verändert werden können, sollte eine Datensicherung auch eine Wiederherstellung zu einem weiter zurückliegenden Zeitpunkt erlauben. Um Datenträgerfehlern vorzubeugen sollten Backups (evtl. rotierend) auf verschiedenen Datenträgern gesichert werden. Lokale Laufwerke Ihres Rechners werden nicht automatisch gesichert!

Unser Angebot: Gemeinsam sollten wir mindestens 1x pro Jahr die Sicherung kontrollieren.

Verweise:

BayLDA - Das Bayerische Landesamt für Datenschutzaufsicht (bayern.de)
> Checkliste Technische und organisatorische Maßnahmen (bayern.de)

Home - IT-Sicherheitscluster e.V.
> (Microsoft Word - 2022-ISA+_Fragenkatalog_öffentlich_3.1.docx) (it-sicherheitscluster.de)

IT-Sicherheit ist eine nicht-delegierbare Chefsache! (security-insider.de)

Auf den Punkt gebracht: IT-Sicherheit gehört zu den Kernaufgaben von Vorstand und Geschäftsführung sowie Aufsichtsrat und Beirat. Beide Führungsgremien sind gesetzlich verpflichtet für ein funktionierendes IT-Risiko- und Sicherheitsmanagement zu sorgen. Damit haben sie bei der Prävention von Cyberattacken eine Schlüsselrolle inne. Sie stehen gemeinsam in der Verantwortung und Haftung. Ihr Engagement ist entscheidend für ein wirksames Cybersecurity-Management. Kurz gesagt: **Cybersecurity ist Chefsache.**