IT-Sicherheitshinweise

Die Pischedda IT-Solutions möchte Ihnen nicht nur wirtschaftliche Produkte anbieten, sondern auch eine datenschutzkonforme und sicherheitstechnisch einwandfreie Umgebung zur Verfügung stellen. Dazu orientieren wir uns an diversen Standards und Rahmenwerken aus dem Bereit des Datenschutzes und der Informationssicherheit.

Neben unseren getroffenen Datenschutz- und Sicherheitsmaßnahmen, welche wir sukzessive dem Stand der Technik entsprechen verbessern, möchten wir Ihnen gerne Hilfen an die Hand geben, mit denen Sie ihre bei uns gemieteten Produkte schützen können.

In den nachfolgenden Ausführungen finden Sie entsprechende Hinweise und Tipps sowie Links zu Organisationen, zu allgemeinen Aspekten aus dem Bereich des Datenschutzes und der Informationssicherheit. Diese Hinweise von uns beziehen sich im Schwerpunkt auf den Teilbereich „IT-Sicherheit / Cyber-Security“ aus der Informationssicherheit.

Cyber-Security Hinweise

Allgemeines

Wenn Sie ein Produkt bei uns mieten, dann haben Sie sich bereits im Vorfeld Gedanken darüber gemacht, wofür Sie dieses Produkt einsetzen wollen. Mit dieser Kenntnis können Sie ihr Produkt absichern. Denn Sie können die Funktionen, die Sie nicht benötigen vielleicht schon im Bereitstellungsprozess (vor der eigentlichen Installation) konfigurieren oder nach der Installation (dies ist abhängig vom jeweiligen Produkt).

Hardening (Systemhärtung)

Ob Anwendung oder Betriebssystem, jeder dieser IT-Produkte sollte so konfiguriert werden, dass diese sicher betrieben werden können. Wenn Sie diese IT-Produkte so bereitstellen, dass diese nur die Funktionen / Services anbieten, die Sie benötigen und nur für die Personen genutzt werden können, für die Sie dieses System vorgesehen haben, dann spricht man von einer sogenannten Systemhärtung (Hardening). Für die populären Anwendungen und Betriebssysteme gibt es bereits hervorragende Hilfen, wie Sie das Hardening durchführen können. Nachfolgend zeigen wir einige gute Quellen auf.

Center for Internet Security, Inc. (CIS®)

Eine gute Anlaufstelle ist das CIS, wenn es um Hardening geht. Es stellt zahlreiche Handreichungen kostenlos (englisch) zum Download zur Verfügung. Es gibt für nahezu alle gängigen Anwenungen und vor allem Betriebssysteme die sogenannten Benchmarks, die Sie nach einer kostenlosen Registrierung herunterladen dürfen.

Diese Benchmarks sind nicht immer für die aktuellste Version (bspw. Debian 12) verfügbar. Wenn dies der Fall sein sollte, dann nutzen Sie einfach die Benchmarks der letzten Version, die Ihnen angeboten werden. In der Regel gibt es in den Versionen nur geringfügige Abweichungen.

Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Eine weitere gute Quelle sind die IT-Grundschutz-Bausteine vom BSI. Hier finden Sie zahlreiche Informationen, die für einen sicheren Betrieb Ihrer Systeme herangezogen werden können. Auch diese Informationen sind kostenlos und liegen zudem in deutscher Sprache vor. Darüber hinaus bietet das BSI auch weitere zahlreiche Publikationen an, die evtl. für das von Ihnen zu härtende Produkt hilfreich sein könnten.

OWASP Foundation

Wenn Sie auch Webanwendungen entwickeln wollen bzw. Ihr WCMS z. B. Wordpress anpassen müssen oder aber auch eine eigene Webanwendung von Grund auf neu entwickeln möchten, dann ist das Open Worldwide Application Security Project (OWASP) auch sehr zu empfehlen. Hier gibt es die berühmte Top 10 Web Application Security Risks Liste, die die häufigsten Risiken bei der Entwicklung von Webanwendungen aufzeigt und es gibt auch Tipps wie man diese vermeiden kann. OWASP bitet auch ein deutsches Chapter an, allerdings finden Sie dort noch nicht alle Projekte in deutscher Sprache.

Produkthersteller und Community Produkte

Auch die Hersteller bspw. Von diversen Linux Distributionen oder auch Microsoft oder VMware bieten zum Teil Hilfen (Hardening Guides) oder ähnliches an.

Checkliste und Tipps & Tricks

Überlegen Sie sich vor der Installation was Sie genau wollen. Neben den Anwendungen / Betriebssystemen werden Sie vermutlich weitere Tools oder Middleware benötigen. Auch Datenbanken kommen häufig zum Einsatz und auch diese Produkte müssen gehärtet werden.

Hier einige Tipps & Tricks:

Weniger ist manchmal mehr

- Installieren Sie nur die Dienste, die Sie benötigen

Updates / Patches

- Halten Sie Ihre System auf dem aktuellen Stand. Also installieren Sie regelmäßig verfügbare Updates. Häufig lassen sich Updates und Patches automatisiert einspielen. Nutzen Sie die Auto-Update Funktionen der Produkte, wenn diese vorhanden sind.

Passwortsicherheit

- Verwenden Sie lange und komplexe Kennwörter mind. 20 Zeichen aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen. Für die Verwaltung und Generierung können Sie einen Passwortmanager nutzen bspw. KeePass oder KeePassXC.
- Denken Sie daran, dass Sie das Master-Passwort für den Passwortmanager auch analog (aufschreiben) und an einen sicheren Ort aufbewahren. Wenn Sie dieses Passwort verlieren, dann können Sie nicht mehr auf Ihre Datenbank mit den Passwörtern zugreifen.
- Sollten Sie bspw. puTTY nutzen, dann bieten sich Zertifikate an. Auch hierzu gibt es gute Tutorials im Netz.
- Nutzen Sie keine Wörter, die in Nachschlagwerken wie bspw. Wörterbüchern stehen. Nutzen Sie Passphrasen.

Berechtigungen und Rollen

- Arbeiten Sie nach Möglichkeit nicht mit dem root / Administrator Benutzer. Legen Sie sich einen neuen User an und nutzen Sie diesen. Fügen Sie den Nutzer bspw. Unter Linux der Gruppe sudoers hinzu.
- Manche System haben Standardbenutzer und Kennwörter. Ändern Sie diese Zugänge direkt noch bevor das System veröffentlicht wird.
- Löschen Sie User, die Sie nicht benötigen.

Backups

- erstellen Sie von Ihren Systemen Backups und das in regelmäßigen Abständen und sichern Sie diese nach Möglichkeit an einem anderen Ort (bspw. Cloudspeicher). Wichtig dabei ist, dass Sie diese Backups zuvor verschlüsseln. Ein gutes Tool ist Duplicati. Für automatisierte verschlüsselte Backups im Serverbereich bietet sich Duplicity an.

Virenschutz

- Auch wenn es in der Cyber-Security als Schlangenöl bezeichnet wird, finden wir den Einsatz von Virenschutzsystemen ein weiteres Mittel zur Verteidigung in der Tiefe. Hier können Sie kostenpflichtige Lösungen einsetzen oder auch was aus der community bspw. ClamAV. Windows Server / Windows 10 reicht der Defender vollkommen aus. Geben Sie hier nicht unnötig Geld aus, sonder investieren Sie dieses sinnvoll bspw. In Speicher für Backups..

Firewall

- Unter Linux und auch Windows ob Desktop oder Server, können Sie die von Hause aus bereits im Betriebssystem zur Verfügung stehenden Firewalls nutzen. In den Paketquellen bei Linux bspw. Ubuntu Server können Sie die Uncomplicated Firewall (UFW) nutzen.
- Bei größeren Infrastrukturen empfehlen wir Ihnen eine dedizierte Firewall und eine Kombination aus mehreren Firewall-Architekturen.

Exploit-Schutz und Anwendungs- und Kernelabsicherung

- Nutzen Sie AppAmor oder SELinux, um Ihre Linux Server noch besser zu schützen. Auch Windows bietet derartige Mechanismen.

Webanwendungen

- Scannen Sie Ihre Webseite mit Tools wie bspw. diesem oder dem hier, um die Sicherheit Ihres Systems zu überprüfen. Noch besser, lassen Sie von Profis Ihre Umgebung auf Herz und Nieren mit einem Pentest prüfen. Alternativ können Sie sich auch mit ParrotOS oder Kali-Linux beschäftigen und Ihre Systeme selbst prüfen.
- Für Wordpress und auch andere WCMS gibt es Security-Plugins (Link) Wir haben diese noch nicht getestet, aber anschauen kann man Sie sich ja mal.