Rundschreiben Datenschutz und Datensicherheit

Sehr geehrte Kolleginnen und Kollegen,

auf Grund des stetig wachsenden Bedrohungspotenzials hinsichtlich Schadsoftware jeglicher Art, haben wir Ihnen im Anhang einige Kernpunkte zur Verbesserung sowie der Aufrechterhaltung des Datenschutzes und der Datensicherheit innerhalb unseres Unternehmens aufgeführt. Da Datenschutz nur bei unternehmensweiter Umsetzung funktionieren kann, beziehen sich die nachfolgenden Punkte sowohl auf administrative Maßnahmen, als auch die Bewusstseinsschärfung des Endbenutzers. Somit bitten wir Sie als administrativ agierende IT-Abteilung, die im Anhang aufgeführten Punkte entsprechend umzusetzen und sofern nötig, die Endbenutzer über einzelne Punkte in Kenntnis zu setzen.

Mit freundlichen Grüßen,
Ihre Datenschutzabteilung

Jonas Fischer, Anna-Lena Hampel, Lukas Jakob, Joshua Jost, Jonathan Köppl

Kriterienkatalog Datenschutz und Datensicherheit

1. **Beachtung eines gewissen Grundschutzes**
   - Verwendung sicherer Passwörter, regelmäßige Änderung der Passwörter
   - Sofern möglich, Verwendung von MFA (Multi-Faktor-Authentifizierung)
   - „Vorsicht statt Nachsicht“

2. **Einschränkung von Userrechten (Rechtesystem)**
   - Installation von Programmen/Treibern blockieren
   - Endbenutzern nur die wirklich notwendigen Rechte gewähren

3. **Aktueller Virenschutz**
   - Systemweiter Virenschutz mit aktuellen Signaturen
   - Zusätzlicher Rollout von Anti-Malware Software
   - Regelmäßige Berichtskontrollen (Konformität, Funde, etc.)

4. **Spam/Junk-E-Mail Schutz auf dem Webserver und den Clients**
   - Mail Protection
   - White-/Blacklisting
   - DDoS-Schutz (Distributed-Denial-of-Service)

5. **Filterregeln Firewall**
   - Potenziell gefährliche Seiten blockieren (Webfilter)
   - Netzwerkzugriff neuer Systeme zunächst blockieren
   - Netzwerkzugriff von außen blockieren

6. **Verschlüsselung**
   - Festplattenverschlüsselung
   - Dateiverschlüsselung
   - Automatische Verschlüsselung von Wechselspeichermedien

7. **Backups**
   - Regelmäßige Erstellung (Intervall je nach Wichtigkeit der Daten)
   - Regelmäßige Testwiederherstellungen, um Datenkonsistenz sicherzustellen
   - Erstellung von Notfallplänen zur Widerherstellung

8. **Sensibilisierung der Nutzer**
   - Nutzer auf potenzielle Gefahren aufmerksam machen (Dateiendungen, Attachements, Phishing Mails)
   - Vorsicht beim surfen (Werbung, Adware)

9. **Auffälligkeiten melden**
   - Endbenutzer dürfen keine Scheu davor haben, sich bei Auffälligkeiten oder sonstigen Fragen an die IT-Abteilung zu wenden

10. **Schulungen**
    - Unterschiedliche Schwerpunkte für Anwender und Administratoren
    - Austausch über aktuelle Bedrohungslage und bereits ergriffene Maßnahmen
    - Anpassung der Maßnahmen an aktuelle Gegebenheiten
    - Aufklärung und Sensibilisierung der Endbenutzer

Jonas Fischer, Anna-Lena Hampel, Lukas Jakob, Joshua Jost, Jonathan Köppl