Handout zum Vortrag vom 16.11.2022 / DigiInfo6 KDLR

Informationssicherheit „Es trifft auch die Kleinen“

Informationssicherheit (be)trifft jeden.

Die fortschreitende Digitalisierung ist für Unternehmen auch mit neuen Risiken verbunden. So wird es zu einer Herausforderung, die immer komplexer werdenden Systeme zu schützen und dabei sowohl gesetzliche als auch branchenspezifische Anforderungen wie IT-Sicherheitsgesetze und EU-Datenschutzverordnungen zu erfüllen.

Anhand der nachfolgenden Fragestellungen können Sie ermitteln, wie Ihr Unternehmen in Sachen IT-Sicherheit aufgestellt ist.

Regelungen für Nutzer/innen

- □ Gibt es klare “Spielregeln” für Ihre Nutzer/innen in Form einer Richtlinie?
- □ Haben Sie die Privatnutzung der IT für die Nutzer/innen klar geregelt?

Awareness

- □ Führen Sie jährlich eine Security Awareness Schulungen durch?
- □ Informieren Sie regelmäßig über neue Bedrohungen auf welche bei der täglichen Arbeit geachtet werden muss?
- □ Führen Sie kontinuierliche Phishing Simulationen um den Umgang mit E-Mail Bedrohungen zu trainieren?

Dokumentation / Notfallhandbuch

- □ Pflegen Sie eine aktuelle IT-Dokumentation, welche für Dritte nachvollziehbar ist?
- □ Pflegen Sie ein aktuelles Notfallhandbuch, sodass im IT-Notfall ein möglichst geregeltes Vorgehen mit konkreten Schritten gewährleistet ist?

IT-Systeme

- □ Führen Sie eine kontinuierliche Inventarisierung Ihrer IT-Systeme (inkl. der mobilen) durch?
- □ Sind alle IT-Systeme mit einem Virenscanner ausgestattet und erkennen Sie falls ein IT-System ohne Virenscanner ist?
- □ Arbeiten Ihre Nutzer/innen ohne lokale Administratoren Rechte?
- □ Wurde die Ausführung von Office Makros per Richtlinie unterbunden?

Netzwerk / Netzübergänge

- □ Wurde die ausgehende Netzwerkkommunikation Richtung Internet auf das notwendige Minimum beschränkt, so dass interne IT-Systeme nicht auf beliebigen Ports mit externen Systemen kommunizieren können?
- □ Wurden Zugriffsregeln für Remote-Benutzer/innen auf das notwendige Minimum beschränkt?
- □ Wird das Firewall Regelwerk Ihrer Unternehmensfirewall regelmäßigen Reviews unterzogen, um Sicherheitsrisiken in der Konfiguration zu erkennen?

DRIMALSKI &Partner

Handout zum Vortrag vom 16.11.2022 / DigiInfo6 KDLR

Informationssicherheit „Es trifft auch die Kleinen“

Informationssicherheit (be)trifft jeden.

Patch Management

- ☐ Setzen Sie für Server und Clients ausschließlich Betriebssysteme ein, welche noch aktuelle Sicherheitsupdates durch den Hersteller erhalten?
- ☐ Stellen Sie die regelmäßige und zeitnahe Installation von Sicherheitsupdates für Server- und Clientbetriebssysteme durch ein geregeltes Verfahren sicher?
- ☐ Stellen Sie die regelmäßige und zeitnahe Installation von Sicherheitsupdates für veröffentlichte Systeme (Firewalls, Exchange Server, Webserver,..) durch ein geregeltes Verfahren sicher?

Privilegierte Konten

- ☐ Sind in Ihren Domänen-Admin und BUILTIN\Administratoren Gruppen ausschließlich Konten für rein administrative Zwecke enthalten und keine Benutzer/innen die für die tägliche Arbeit mit E-Mail und Internet verwendet werden?
- ☐ Haben Sie für Serverdienste dedizierte Dienstkonten implementiert (z.B. Backup), so dass der BUILTIN\Administrator von jeglichen Abhängigkeiten entbunden wurde?
- ☐ Nutzen alle administrativen Konten ausreichend sichere (20 Stellen) und individuelle Kennwörter?
- ☐ Nutzen Sie zur Administration (Active Directory, Server, Firewall, Cloud,..) personalisierte Admin-Konten (z.B. admin-mustermann)?

Mobiles Arbeiten

- ☐ Wird Remote-Arbeit von privaten Endgeräten der Nutzer/innen durchgeführt?
- ☐ Sind Firmen-Laptops und Smartphones durch eine Verschlüsselung geschützt, so dass gespeicherte Informationen bei Verlust eines Gerätes nicht in die Hände Dritter geraten?
- ☐ Werden mobile Firmen-Laptops und Smartphones ebenso regelmäßig mit Sicherheitsupdates versorgt wie interne IT-Systeme?

Datensicherung

- ☐ Werden Speicherorte (z.B. Fileserver), Serverbetriebssysteme und Serveranwendungen so gesichert werden, dass ihr letzter vollständig wiederherstellbarer Zustand nicht älter als 24 Stunden ist?
- ☐ Führen Sie Datensicherungen nach dem Mehr-Generationen-Prinzip durch (Tages-, Wochen- und Monatsbackups)?
- ☐ Haben Sie Backupmaßnahmen getroffen (Duplizierung, Auslagerung,..), um gesicherte Daten vor Schadensereignissen (Feuer, Wasser,..) zu schützen?
- ☐ Haben Sie Maßnahmen getroffen, um die Ausbreitung von Schadsoftware (z.B. Verschlüsselungstrojaner) auf Ihre Backupserver und gesicherten Daten zu verhindern?
- ☐ Führen Sie regelmäßige Wiederherstellungstests für einzelne Dateien, sowie für gesamte Serversysteme durch?

DRIMALSKI &Partner

Handout zum Vortrag vom 16.11.2022 / DigiInfo6 KDLR

Informationssicherheit „Es trifft auch die Kleinen“

Informationssicherheit (be)trifft jeden.

E-Mail

- ☐ Blockiert Ihr E-Mail Gateway von extern eingelieferte ausführbare E-Mail Anhänge und Skript-Dateien?
- ☐ Erkennt und blockiert Ihr E-Mail Gateway eingelieferte E-Mail Anhänge, die Office Makros enthalten (in Office Formaten ab 2007 aber auch in Legacy Office Formaten wie .doc / .xls)?
- ☐ Wenden Sie vor der Zustellung von E-Mail Anhängen aktuelle Sandboxing Verfahren an?
- ☐ Blockieren Sie eingelieferte E-Mails, welche Ihre eigene Unternehmensdomäne im E-Mail Envelope vortäuschen?
- ☐ Blockieren Sie eingelieferte E-Mails, welche Ihre eigene Unternehmensdomäne im E-Mail Header vortäuschen?
- ☐ Nutzen Sie die E-Mail Authentication Verfahren SPF, DKIM und DMARC für Ihre eigenen Domänen & wenden Sie auch zur Prüfung eingehender E-Mails an?

Web-Zugriffe

- ☐ Setzen Sie SSL Scanning für Web-Zugriffe ein, um Downloads schadhafter/unerlaubter Dateien aus dem Internet auch in verschlüsselten HTTPs Verbindungen zu erkennen?
- ☐ Blockieren Sie den Download ausführbarer Dateien / Skript Dateien (z.B. Powershell) aus dem Internet?
- ☐ Blockieren Sie den Download von Dateien aus dem Internet, die Office Makros enthalten (sowohl in Office Formaten ab 2007, als auch in Legacy Office Formaten wie .doc /.xls)?

Zugänge und Benutzerkennwörter

- ☐ Stellen Sie eine angemessene Mindestlänge Ihrer Kennwörter sicher (z.B. 12 Zeichen)?
- ☐ Unterbinden Sie die Vergabe von Active Directory / Azure AD Kennwörtern, welche bereits in einem Datenleck enthalten waren (und somit als kompromittiert gelten)?
- ☐ Erzwingen Sie für alle nach extern veröffentlichten Dienste (Webmail, VPN, Portale, etc.) Multifaktor Authentisierung?

DRIMALSKI &Partner

Drimalski & Partner GmbH
Ortesweg 11 | 36043 Fulda

Tel. 0661 / 90 20 30 | www.drimalski.de