Unter Cyberangreifenden und Administrierenden

IT-Verantwortlicher einer deutschen Kommune (Symboldbild)

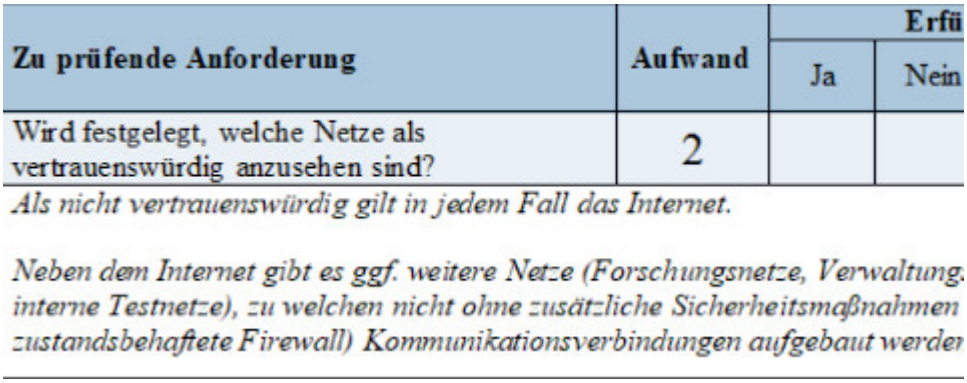
Ich habe mir die 18 Checklisten des BSI angesehen, auf die Heise hinwies: „Kommunen sind zunehmend Ziele von Cyber-Angriffen. Für angemessenen Schutz mangelt es oft an Wissen und Personal."

Da bin ich aber gespannt. Wie sollen die Kommunen das ändern, wenn sie ohnehin für nichts mehr Geld haben? Fortbildungskurse für Mitarbeiter? Wer soll das bezahlen?

Man kann natürlich über alles meckern. Wenn man sich ansieht, was das BSI vorschlägt, beginnt man zu ahnen, wie es in den Kommunen cybermäßig aussieht. Word-Dokumente! Da fängt es schon an. Das BSI geht mit schlechtem Beispiel voran. Da fällt mir die uralte Schlagzeile ein. „Microsoft Word bytes Tony Blair in the butt".

Schon gelesen, BSI? *Microsoft warnt Kunden aktuell vor einer gravierenden Sicherheitslücke in Verbindung mit docx-Dateien. Das Gefährliche an dieser Sicherheitslücke ist die Tatsache, dass das alleinige Öffnen der jeweiligen Word-Datei genügt, um den Schadcode auszuführen und Remote Code Execution zu*

ermöglichen.



Zu prüfende Anforderung	Aufwand	Erfü	
		Ja	Nein
Wird festgelegt, welche Netze als vertrauenswürdig anzusehen sind?	2		

Als nicht vertrauenswürdig gilt in jedem Fall das Internet.

Neben dem Internet gibt es ggf. weitere Netze (Forschungsnetze, Verwaltung. interne Testnetze), zu welchen nicht ohne zusätzliche Sicherheitsmaßnahmen zustandsbehaftete Firewall) Kommunikationsverbindungen aufgebaut werde

Der Transport von Dokumenten und Datenträgern sollte bspw. in einer verschlossenen Tasche und/oder im Kofferraum eines Fahrzeugs erfolgen, statt sie sichtbar und leicht zugreifbar zu machen.
Full ack. Man ist von lokalen Politikern gewohnt, dass sie Laptops mit unverschlüsselten Daten gern in Fahrzeugen lassen und dass diese Laptops dann bei Rockerbanden landen. Das sollten Kommunen anders handhaben.

Ist festgelegt, ob und wie dienstliche Informationen auf fremden IT-Systemen verarbeitet werden dürfen?
Gilt das nicht viel mehr für das Gegenteil? Also etwa während der Dienstzeit Raubkopien herstellen – verboten oder nicht? Und was ist ein „fremdes“ IT-System? Bei mir wäre da Microsoft erste Wahl für Alienmäßiges. (Chor der Administrierenden im Hintergrund: Aber was ist dann mit der Cloud?)

Zielsetzung ist der Bezug von integrer Software, die bei einem seriösen Anbieter gekauft/heruntergeladen wird. Eine vertrauenswürdige Quelle ist typischerweise der Hersteller/Entwickler der jeweiligen Software. Idealerweise stellt die vertrauenswürdige Quelle eine Möglichkeit bereit, die Software auf Integrität zu überprüfen. Steht diese Möglichkeit zur Verfügung, sollte sie auch genutzt werden.
„Integer“ ist nur und ausschließlich Open-Source-Software, hilfsweise Software, die von Edward Snowden oder Phil Zimmermann persönlich empfohlen wurde. Aber dann bliebe in den Kommunen vermutlich gar nichts mehr übrig von der schönen

Klickibunti-Welt. Auch Netzwerk Recherche ist im April 2023 mit dem Newsletter auf diesen Zug aufgesprungen. Wenn schon Journalisten einen feuchten Kehricht auf Sicherheit geben, was sollen dann die Kommunen machen?

Aktive Inhalte in Office-Dokumenten sollten nie automatisch ausgeführt werden. Falls eine händische Ausführung notwendig ist, müssen die aktiven Inhalte aus vertrauenswürdigen Quellen stammen. Alle Benutzenden [sic] müssen bezüglich der Gefährdungen durch Aktive Inhalte in Office-Dateien sensibilisiert werden. Zu Office-Anwendungen zählen hier insbesondere auch Anwendungen für PDF-Dateien sowie E-Mail-Clients.
Die Botschaft hör ich wohl, allein mir fehlt der Glaube. Wieso eigentlich „händisch“? Oder meinen die „händisch sensibilisieren“? Das würde mich interessieren, obzwar es dann auf die einzelne Verwaltungsfachangestellte ankäme. Zwischenfrage, wie vor Sodom und Gomorrha: Gibt es Kommunen, die als E-Mail-Client *nicht* Outlook einsetzen?

Zudem sollte der Versand und Empfang von ausführbaren Dateien über E-Mail, die Nutzung veralteter Office-Formate (z. B. .doc oder .xls) oder das lokale Ausführen von Skripten nach Möglichkeit blockiert werden.
Schon klar. Aber ist das Verschicken von Attachments mit Visual Basic Script nicht so was von Anfang des Jahrtausends?

Es sollten ausschließlich moderne Webbrowser mit Sicherheitsfunktionen und mit aktueller Herstellerunterstützung verwendet werden.
Definieren sie „modern“?1 Ich darf also weder den Netscape Navigator noch Lynx einsetzen? Was erlauben BSI?


Bundesamt für Sicherheit in der Informationstechnik

Stand: 24.07.2023

Checkliste:
Vorbereitung für Sicherheitsvo

Deutschland Digital•Sicher•BSI•

Zugrundeliegende Bausteine (IT-Grundschutz-Kompendium 2022):

- DER.2.1 Behandlung von Sicherheitsvorfällen

Bearbeitungsinformationen

Hier bitte das/die betrachtete(n) Zielobjekt(e) einfügen.

Die Prüfung sollte bereits auf dem E-Mail-Server stattfinden. Es muss dabei geregelt werden, wie mit Dateien umgegangen werden soll, die das Schutzprogramm nicht lesen kann, z. B. bei verschlüsselten Daten. Falls die Prüfung nicht auf dem E-Mail-Server stattfinden kann, muss sie auf dem E-Mail-Client erfolgen.
Außerdem sollten folgende Maßnahmen umgesetzt werden:
Ausführbare Dateien in E-Mail-Anhängen unterbinden
Prüfung des Dateiformats (Anzeige der Dateiendungen in voller Länge aktivieren)
Größe von Dateianhängen beschränken (der Wert kann bspw. individuell je nach vorhandenen Ressourcen, Fachverfahren oder externen Vorgaben festgelegt werden)
Ja, das ist doch die Frage: Wie soll man mit verschlüsselten Daten umgehen? Alles so lassen oder gar entschlüsseln? Nennen Sie mir *eine* Kommune in Deutschland, der man eine verschlüsselte Nachricht schicken kann! Eine! Nur eine! Wait a minute. Welches „Schutzprogramm“ kann verschlüsselte Daten nicht lesen? Sollte das nicht auch verboten werden?

Soweit sinnvoll und möglich sollte auch die automatische Darstellung von HTML-Inhalten deaktiviert werden.
Ja! Full ack. Es geschehen noch Zeichen und Wunder. Aber die Firma möchte ich sehen, die ihren Angestellten die E-Mails auf *plain text* umstellt. Und die meisten wissen gar nicht, was ich damit meine. Noch nicht einmal der Deutsche Journalistenverband macht das.

Nur berechtigte Benutzende [sic] sollten sich an Clients anmelden können. Es gibt verschiedene Techniken, über die die Authentizität von Benutzenden nachgewiesen werden kann. Die bekanntesten sind: PINs (Persönliche Identifikationsnummern), Passwörter, Token wie z. B. Zugangskarten sowie Biometrie.
Ich sage nur: Paxton! Ich schreibe gerade ein Handbuch, wie man damit Zugangskarten programmiert und druckt, weil Paxton keines herausrückt, sondern die Experten lieber zu Schulungen einlädt, damit das Herrschaftswissen kostenpflichtig bei ihnen bleibt.

Benutzende [sic] sollten angehalten werden, die Bildschirmsperre bei Verlassen des Arbeitsplatzes zu aktivieren.
Ich verrate jetzt kein Betriebsgeheimnis, aber in meiner Firma ist jeder Angestellter verpflichtet, den Bildschirm zu sperren, sobald er oder sie den Allerwertesten auch nur ein wenig lüftet.

Nur Administrierende [sic] sollten von externen Speichermedien booten können.
Ähm. Das ist irgendwo erlaubt? Normale Nutzer dürfen von USB-Sticks booten?

Administrierende müssen außerdem über eine geeignete Persönlichkeit verfügen, um die ihnen übertragenen Aufgaben zuverlässig und sorgfältig zu erledigen.
Wie und zu welchem Ende erlangt man eine „geeignete Persönlichkeit“? Und wer stellt einem dann das betreffende Zertifikat aus?

Ist sichergestellt, dass Benutzende einem Zugriff auf ihre Desktop-Umgebung zwecks Fernwartung jeweils aktiv zustimmen müssen?
Das muss man extra betonen? Ich werde also manchmal in einer Kommune ferngewartet, ohne dass ich es weiß? Das stelle ich mir für Politiker nützlich vor, aber doch nicht für IT-Systeme?

Die Personal Firewall muss so konfiguriert werden, dass die Benutzenden [sic] nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können.
Das wird jetzt Comedy. 0x8007042c? ChatGPT: *Die Zeichenfolge „0x8007042c“ ist ein Fehlercode im hexadezimalen Format. In Windows-Betriebssystemen werden solche Fehlercodes oft verwendet, um spezifische Probleme oder Fehlerzustände zu identifizieren. In diesem Fall steht der Fehlercode „0x8007042c“ für den Windows-Firewall-Fehler „RPC-Server nicht verfügbar“.* Aha.

Die Aufgaben sollten so verteilt werden, dass einerseits Überschneidungen in den Zuständigkeiten vermieden werden und andererseits keine Lücken entstehen.
Rharbarber, Rharbarber, Rahfasel. Man ahnt: Wenn mehr als einer zuständig ist, geht gar nichts mehr. Und meistens ist niemand zuständig. IT-Standort Deutschland at its best.

Virenschutzprogramme, die E-Mails entschlüsseln (Symbolbild)

Fehlende Kenntnis über den Speicherort von Informationen. Unbefugter Zugriff auf Informationen, z. B. durch Administratoren des Cloud-Diensteanbieters.
Keine Ahnung. Sollte denn eine Kommune wissen, wo in der Microsoft-Wolke ihrer geheimen Daten gespeichert hat sind und wer die verwaltet? Seriously? Und an wen sollen die faxen, um das zu erfahren?

Passwörter müssen geheim gehalten werden.
Gut zu wissen. Ich kenne ein großen Krankenhaus in Berlin, bei dem an der Rezeption das Master-Passwort des Rechners an dessen Monitor klebt. Lächerlich ist dieser Hinweis gar nicht.

Eine erzwungene Passwort-Erneuerung ist wenig zielführend, da dies zur Nutzung einfacher Passwörter nach einem festen Muster verleitet.
Ich werde in unregelmäßigen Abständen von der IT-Abteilung in sehr höflichem sophisticated business English aufgefordert, mein Passwort zu ändern. Falls ich das nicht mache, wird mein Account gesperrt. Ich benutze trotzdem keine einfachen Passwörter. Das wird lustig, wenn dieses deutsche Sonderzeichen enthält, man aber – wie ich – mit einer englischen Tastatur arbeiten muss oder mit einer deutschen Tastatur, die Englisch belegt ist – und man nur drei Versuche hat, das Passwort einzugeben.

Gibt es eine Festlegung, wie mit verschlüsselten E-Mails zu verfahren ist, wenn diese nicht durch das Virenschutzprogramm entschlüsselt werden können?
WTF, BSI? Virenschutzprogramme, die E-Mails entschlüsseln?