Vervielfältigung und Verbreitung

Dies ist ein Werk der ISi-Reihe. Ein vollständiges Verzeichnis der erschienenen Bände finden Sie auf den Internet-Seiten des BSI.

https://www.bsi.bund.de/ISi-Reihe

Bundesamt für Sicherheit in der Informationstechnik
ISi-Projektgruppe
Postfach 20 03 63
53133 Bonn
Tel. +49 (0) 228 99 9582-0
E-Mail: isi@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Der vorliegende Checklisten-Katalog richtet sich vornehmlich an Administratoren und Sicherheitsrevisoren, die mit der Einrichtung, dem Betrieb und der Überprüfung einer Infrastruktur zur sicheren Nutzung von Web-Angeboten befasst sind.

1.1 Funktion der Checklisten

Die Checklisten fassen die relevanten Empfehlungen der BSI-Studie *Sichere Nutzung von Web-Angeboten* [ISi-Web-Client] in kompakter Form zusammen. Sie dienen als Anwendungshilfe, anhand derer die Umsetzung der in der Studie beschriebenen Sicherheitsmaßnahmen im Detail überprüft werden kann.

Die Kontrollfragen dieser Checkliste beschränken sich auf produktspezifische Empfehlungen für den Microsoft Internet Explorer (im weiteren Dokument als „Internet Explorer“ bezeichnet) im Kontext des ISi-Web-Client-Moduls. Die zur Zeit der Entstehung dieser Studie verfügbare stabile Version des Microsoft Internet Explorers diente als Basis für die folgende Checkliste. Es handelte sich dabei um den Microsoft Internet Explorer 11 Desktop-Version in deutscher Sprache. Allgemeine Grundschutzmaßnahmen, die nicht spezifisch für die Verwendung des Internet Explorers sind, werden von den Fragen nicht erfasst. Solche grundlegenden Empfehlungen sind der allgemeinen generischen Checkliste (ISi-Check-gen zu ISi-Web-Client) und den BSI-Grundschutzkatalogen [ITGSK] zu entnehmen. Die Grundschutzkataloge bilden das notwendige Fundament für ISi-Check. Auch Prüffragen, die bereits durch die Checkliste zur BSI Studie *Sichere Anbindung lokaler Netze an das Internet* [ISi-LANA] abgedeckt wurden, werden hier nicht wiederholt.

Die Checklisten wenden sich vornehmlich an IT-Fachleute. Die Anwendung von ISi-Check setzt vertiefte Kenntnisse auf dem Gebiet der IP-Netze, der Administration von Betriebssystemen und der IT-Sicherheit voraus. Die Kontrollfragen ersetzen *nicht* ein genaues Verständnis der technischen und organisatorischen Zusammenhänge beim Betrieb einer Infrastruktur zur sicheren Nutzung von Web-Angeboten. Nur ein kundiger Anwender ist in der Lage die Prüfaspekte in ihrem Kontext richtig zu werten und die korrekte und sinnvolle Umsetzung der abgefragten Empfehlungen in Einklang mit den allgemeinen Grundschutzmaßnahmen zu bringen.

Der Zweck der Kontrollfragen besteht also vor allem darin, dem Anwender bei der der Konfiguration des Microsoft Internet Explorers die erforderlichen Maßnahmen und die dabei verfügbaren Varianten übersichtlich vor Augen zu führen. Die Checklisten sollen gewährleisten, dass kein wichtiger Aspekt vergessen wird.

1.2 Benutzung der Checklisten

Der ISi-Reihe liegt ein übergreifender Ablaufplan zugrunde, der im Einführungsdokument [ISi-E] beschrieben ist. Die Checklisten des ISi-Web-Client-Moduls haben darin ihren vorbestimmten Platz. Vor Anwendung der Checklisten muss sich der Anwender mit dem Ablaufplan [ISi-E] und mit den Inhalten der ISi-Web-Client-Studie vertraut machen. Um die Kontrollfragen zu den verschiedenen Prüfaspekten zu verstehen und zur rechten Zeit anzuwenden, ist die genaue Kenntnis dieser Dokumente erforderlich.

Die Checklisten fragen die relevanten Sicherheitsempfehlungen der vorliegenden Studie ab, ohne diese zu begründen oder deren Umsetzung näher zu erläutern. Anwender, die den Sinn einer Kontrollfrage nicht verstehen oder nicht in der Lage sind, eine Kontrollfrage sicher zu beantworten,

können vertiefende Informationen in der Studie nachschlagen. IT-Fachleute, die mit der Studie bereits vertraut sind, sollten die Kontrollfragen in der Regel jedoch ohne Rückgriff auf die Studie bearbeiten können.

Format der Kontrollfragen

Alle Kontrollfragen sind so formuliert, dass die erwartete Antwort ein JA ist. Zusammenhängende Kontrollfragen sind – soweit sinnvoll – hierarchisch unter einer übergeordneten Frage gruppiert. Die übergeordnete Frage fasst dabei die untergeordneten Kontrollfragen so zusammen, dass ein Bejahen aller untergeordneten Kontrollfragen ein JA bei der übergeordneten Kontrollfrage impliziert.

Bei hierarchischen Kontrollfragen ist es dem Anwender freigestellt, nur die übergeordnete Frage zu beantworten, soweit er mit dem genannten Prüfaspekt ausreichend vertraut ist oder die Kontrollfrage im lokalen Kontext nur eine geringe Relevanz hat. Die untergeordneten Fragen dienen nur der genaueren Aufschlüsselung des übergeordneten Prüfkriteriums für den Fall, dass sich der Anwender unschlüssig ist, ob die betreffende Vorgabe in ausreichendem Maße umgesetzt ist. Die hierarchische Struktur der Checklisten soll dazu beitragen, die Kontrollfragen effizient abzuarbeiten und unwichtige oder offensichtliche Prüfaspekte schnell zu übergehen.

Iterative Vorgehensweise

Die Schachtelung der Kontrollfragen ermöglicht auch eine iterative Vorgehensweise. Dabei beantwortet der Anwender im ersten Schritt nur die übergeordneten Fragen, um sich so einen schnellen Überblick über potenzielle Umsetzungsmängel zu verschaffen. Prüfkomplexe, deren übergeordnete Frage im ersten Schritt nicht eindeutig beantwortet werden konnte oder verneint wurde, werden im zweiten Schritt priorisiert und nach ihrer Dringlichkeit der Reihe nach in voller Tiefe abgearbeitet.

Normaler und hoher Schutzbedarf

Alle Kontrollfragen, die nicht besonders gekennzeichnet sind, beziehen sich auf obligatorische Anforderungen bei normalem Schutzbedarf. Diese müssen bei hohem Schutzbedarf natürlich auch berücksichtigt werden. Soweit für hohen Schutzbedarf besondere Anforderungen zu erfüllen sind, ist der entsprechenden Kontrollfrage ein „**[hoher Schutzbedarf]**“ zur Kennzeichnung vorangestellt. Bezieht sich die Frage auf einen bestimmten Sicherheits-Grundwert mit hohem Schutzbedarf, so lautet die Kennzeichnung entsprechend dem Grundwert zum Beispiel „**[hohe Verfügbarkeit]**“. Anwender, die nur einen normalen Schutzbedarf haben, können alle so gekennzeichneten Fragen außer Acht lassen.

Varianten

Mitunter stehen bei der Umsetzung einer Empfehlung verschiedene Realisierungsvarianten zur Wahl. In solchen Fällen leitet eine übergeordnete Frage den Prüfaspekt ein. Darunter ist je eine Kontrollfrage für jede der möglichen Umsetzungsvarianten angegeben. Die Fragen sind durch ein „**– oder –**“ miteinander verknüpft. Um das übergeordnete Prüfkriterium zu erfüllen, muss also mindestens eine der untergeordneten Kontrollfragen bejaht werden.

Befinden sich unter den zur Wahl stehenden Kontrollfragen auch Fragen mit der Kennzeichnung „**[hoher Schutzbedarf]**“, so muss mindestens eine der so gekennzeichneten Varianten bejaht werden, um das übergeordnete Prüfkriterium auch bei hohem Schutzbedarf zu erfüllen.

2 Konzeption

In der Konzeptionsphase des Ablaufplans gemäß [ISi-E] müssen eine sichere Netzarchitektur erstellt und organisatorische Aspekte beachtet werden. Die Konzeptionsphase erfolgt vor der Auswahl der sicheren Komponenten bzw. deren Konfiguration und Betrieb.

Da diese Phase bereits abgeschlossen sein sollte, bevor der Microsoft Internet Explorer für die Nutzung von Web-Angeboten konfiguriert wird, behandelt diese produktspezifische Checkliste die Konzeption nicht erneut im Detail.

2.1 Client-PCs

☐ Sind die lokalen Benutzerrechte, mit denen der Internet Explorer vom Arbeitsplatz aus gestartet wird, dem Schutzbedarf angemessen? Das heißt:

- o Wird der gleiche Benutzer für interne Tätigkeiten und für die Web-Nutzung verwendet?
  – oder –
- o Wird der Internet Explorer mit den Rechten eines eigenen Benutzers gestartet, der keine Rechte auf interne Informationen besitzt und ausschließlich zur Web-Nutzung verwendet wird?

☐ Werden den Benutzern auf internen Clients geeignet konfigurierte Internet Explorer-Installationen für die Nutzung von Web-Angeboten zur Verfügung gestellt?

☐ Wird verhindert, dass die vom Administrator getroffenen Einstellungen von Benutzern verändert werden können?

3 Auswahl sichererer Komponenten

Auf die Konzeptionsphase folgt die Phase der Realisierung und Auswahl der sicheren Komponenten laut [ISi-E]. Da dieser Abschnitt bereits abgeschlossen sein sollte, bevor der Microsoft Internet Explorer konfiguriert wird, behandelt diese produktspezifische Checkliste diese Phase nicht erneut.

4 Konfiguration

Nach der Beschaffung der benötigten Komponenten erfolgt deren Konfiguration durch die Administratoren. Der folgende Abschnitt enthält die für eine sichere Konfiguration zu berücksichtigenden Punkte.

Die zur Zeit der Entstehung dieser Studie verfügbare stabile Version des Microsoft Internet Explorers diente als Basis für die folgende Checkliste. Es handelte sich dabei um den Microsoft Internet Explorer 11 Desktop-Version in deutscher Sprache.

Der Internet Explorer bietet die Auswahl zwischen unterschiedlichen voreingestellten Sicherheitsstufen. Sofern eine bestimmte Stufe für eine Zone vorausgesetzt wird, ist dies explizit in der Checkliste vermerkt. Sollten weitere Einstellungen abgefragt werden, handelt es sich dabei um Abweichungen von der Standardkonfiguration für die jeweilige Sicherheitsstufe. **Einstellungen, die bereits in den Standardeinstellungen auf einen sicheren Wert vorkonfiguriert sind, werden von der Checkliste nicht explizit abgefragt. Bei bereits bestehenden Systeme können diese Standardeinstellungen über den Menüpunkt Extras / Internetoptionen / Erweitert / Zurücksetzen wiederhergestellt werden.**

Die Reihenfolge der Menüpunkte in den Fragen entspricht genau der Bedienungsreihenfolge im Browser. Die einzelnen Menü-Optionen bzw. -Ebenen sind dabei durch Schrägstriche („/“) voneinander getrennt. Die Namen von spezifischen Optionen und deren Werte werden stets unter Anführungszeichen gesetzt (zum Beispiel: „Option“ auf „Aktivieren“ gesetzt).

Für nähere Informationen zu den angeführten Fragestellungen wird auf die BSI Studie [ISi-Web-Client] verwiesen.

4.1 Client-PCs

Ein Großteil der Web-Nutzung findet von den Client-PCs der Mitarbeiter statt. Gleichzeitig befinden sich die Clients jedoch im internen Netz, sodass eine Kompromittierung gravierende Auswirkungen für die Verfügbarkeit, die Vertraulichkeit und die Integrität der Informationen der Institution haben kann. Aus diesem Grund ist es wichtig, die Komponenten richtig zu konfigurieren, um ein möglichst geringes Restrisiko zu erreichen.

Betriebssystemeinstellungen

Da der Internet Explorer auf unterschiedlichen Versionen des Microsoft Windows-Betriebssystems betrieben werden kann, wird auf dieses nicht explizit eingegangen. Es werden jedoch Eigenschaften für das Betriebssystem vorausgesetzt, die in der Studie [ISi-Web-Client] spezifiziert sind und in der generischen Checkliste abgefragt werden.

- ☐ Wird bei der Installation und bei der Konfiguration des Internet Explorers auf Clients im internen Netz das Minimalprinzip beachtet?
  - ☐ *Wird nur unbedingt benötigte Erweiterungssoftware installiert?*
  - ☐ *Arbeiten die Benutzer mit eingeschränkten Rechten (d. h. nicht mit Administratoren-Rechten)?*

Konfiguration der Personal Firewall

☐ Sind erlaubte Verbindungen zu Web-Angeboten an die Verwendung des Internet Explorers gebunden?

Sicherheitseinstellungen für Browser

☐ Erfolgt die Verwaltung vom Internet Explorer zentral?

☐ Ist unter dem Menüpunkt *Extras / Internetoptionen / Verbindungen / LAN-Einstellungen* die Proxy-Konfiguration gemäß den Einstellungen für das Application-Level-Gateway angepasst?

☐ Ist unter dem Menüpunkt *Extras / Internetoptionen / Datenschutz* die Check-Box „Nie zulassen, dass Websites Ihren physischen Standort anfordern“ auf „Aktivieren“ gesetzt?

☐ Ist unter *Extras / Add-Ons verwalten / Suchanbieter* die Option „In Adressleiste suchen“ deaktiviert?

☐ Ist unter *Extras / Internetoptionen / Inhalte / AutoVervollständigen / Einstellungen / AutoVervollständigen verwenden für* auch die Check-Box „Windows Search für bessere Suchergebnisse“ deaktiviert?

☐ Ist unter *Extras / Internetoptionen / Inhalte / AutoVervollständigen / Einstellungen / AutoVervollständigen verwenden für* auch die Check-Box „Vorschlagen von URLs“ deaktiviert?

☐ Sind unter dem Menüpunkt *Extras / Internetoptionen / Sicherheit* für die Zone „Internet“ die Standardeinstellungen der Stufe „Hoch“ ausgewählt?

☐ Ist unter dem Menüpunkt *Extras / Internetoptionen / Sicherheit / Zone „Internet“ / Stufe anpassen / Downloads* die Option „Dateidownload“ auf „Aktivieren“ gesetzt?

☐ Ist unter dem Menüpunkt *Extras / Internetoptionen / Sicherheit* / Zone „Internet“ */ Stufe anpassen / Verschiedenes* die Option „SmartScreen-Filter verwenden“ auf „Deaktivieren“ gesetzt?

☐ Sind unter dem Menüpunkt *Extras / Internetoptionen / Sicherheit* für die Zone „Vertrauenswürdige Sites“ die Standardeinstellungen der Stufe „Mittel bis hoch“ ausgewählt?

☐ Ist unter dem Menüpunkt *Extras / Internetoptionen / Sicherheit* / Zone „Vertrauenswürdige Sites“ */ Stufe anpassen / Verschiedenes* die Option „SmartScreen-Filter verwenden“ auf „Deaktivieren“ gesetzt?

☐ Ist unter dem Menüpunkt *Extras / Internetoptionen / Erweitert* unter den Einstellungen „Sicherheit” die Check-Box „SmartScreen-Filter aktivieren“ deaktiviert?

☐ Ist unter dem Menüpunkt *Extras / Internetoptionen / Sicherheit / Zone „ Vertrauenswürdige Sites“* unter „Sicherheitsstufe für diese Zone“ die Option „Geschützten Modus aktivieren“ aktiviert?

☐ Ist unter dem Menüpunkt *Extras / Internetoptionen / Erweitert* unter „Sicherheit“ die Option „Erweiterten geschützten Modus aktivieren“ aktiviert?

☐ Sind unter dem Menüpunkt *Extras / Internetoptionen / Sicherheit* / Zone „Vertrauenswürdige Sites“ */ Stufe Anpassen / ActiveX-Steuerelemente und Plug-Ins* die ActiveX-Steuerelemente deaktiviert?

- ☐ *Ist die Option „ActiveX-Steuerelemente ausführen, die als "sicher für Skripting" markiert sind“ deaktiviert?*
- ☐ *Ist die Option „ActiveX-Steuerelemente und Plug-Ins ausführen“ deaktiviert?*

- ☐ *Ist die Option „Binär- und Skriptverhalten“ deaktiviert?*
- ☐ Ist unter dem Menüpunkt *Extras / Internetoptionen / Sicherheit / Zone „Vertrauenswürdige Sites“ / Stufe anpassen / Verschiedenes / Websites, die sich in Webinhaltzonen niedriger Berechtigung befinden, können in diese Zone navigieren die Option „Deaktivieren“ gewählt?*

☐ Ist die maximale Anzahl an Tagen, für die die Chronik gespeichert wird, im Menüpunkt *Extras / Internetoptionen / Allgemein / Browserverlauf / Einstellungen / Verlauf* definiert und auf allen Clients konfiguriert?

☐ **[hoher Schutzbedarf]** Werden private Daten wie Verlauf, Cookies und temporäre Dateien beim Beenden bzw. Neustart des Browsers gelöscht?

- o Wird im privaten Modus (InPrivate) gearbeitet? (Anmerkung: Durch „iexplore.exe -private“ ist es möglich den Internet Explorer im InPrivate-Modus zu starten) **– oder –**
- o Ist unter dem Menüpunkt *Extras / Internetoptionen / Allgemein / Browserverlauf* die Option „Browserverlauf beim Beenden löschen“ aktiviert?

☐ **[hohe Integrität]** Ist der Browser-Cache deaktiviert?

- ☐ *Ist unter dem Menüpunkt Extras / Internetoptionen / Allgemein / Browserverlauf / Einstellungen / Temporäre Internetdateien / Neuere Versionen der gespeicherten Seiten suchen die Option „Bei jedem Zugriff auf die Webseite“ ausgewählt?*
- ☐ *Ist unter dem Menüpunkt Extras / Internetoptionen / Allgemein / Browserverlauf / Einstellungen / Temporäre Internetdateien der Zähler „Zu verwendender Speicherplatz“ auf den niedrigsten möglichen Wert gesetzt?*
- ☐ *Ist unter dem Menüpunkt Extras / Internetoptionen / Erweitert / Sicherheit die Check-Box bei der Option „Leeren des Ordners für temporäre Internetdateien beim Schließen des Browsers“ aktiviert?*
- ☐ *Ist unter dem Menüpunkt Extras / Internetoptionen / Erweitert / Sicherheit die Check-Box bei der Option „Verschlüsselte Seiten nicht auf dem Datenträger speichern“ aktiviert?*

☐ Entsprechen die installierten Plug-Ins und Add-Ons unter dem Menüpunkt *Extras / Internetoptionen / Programme / Add-Ons verwalten* dem Minimalprinzip?

☐ Werden gespeicherte Authentisierungsmerkmale ausreichend geschützt?

- ☐ *Ist unter dem Menüpunkt Extras / Internetoptionen / Inhalte / AutoVervollständigen / Einstellungen / AutoVervollständigen verwenden für die Check-Box „Benutzernamen und Kennwörter für Formulare“ abgewählt?*
- ☐ *Kommen zum Speichern von Benutzernamen und Passwörtern externe Programme zum Einsatz, welche diese Authentisierungsmerkmale mit einem sicheren Passwort verschlüsseln?*

☐ Werden die Benutzer vor Webseiten mit nicht vertrauenswürdigen Zertifikaten geschützt?

- ☐ *Sind im Menüpunkt Extras / Internetoptionen / Inhalte / Zertifikate / Vertrauenswürdige Stammzertifizierungsstellen lediglich vertrauenswürdige Zertifizierungsstellen für Server-Zertifikate eingetragen (im Normalfall sollten nur die Zertifizierungsstellen für Zertifikate des Proxys und interner Server akzeptiert werden)?*
- ☐ *Erfolgt die Verwaltung der zulässigen Zertifizierungsstellen zentral?*
- ☐ *Wird verhindert, dass Benutzer zusätzliche Zertifizierungsstellen hinzufügen?*

- ☐ Wird verhindert, dass Web-Angebote mit Hilfe von Cookies detaillierte Profile über Benutzer erstellen können?
  - ☐ *Ist unter Extras / Internetoptionen / Datenschutz / Erweitert die Check-Box „Automatische Cookie Behandlung außer Kraft setzen“ aktiviert?*
  - ☐ *Ist unter Extras / Internetoptionen / Datenschutz / Erweitert / Cookies von Drittanbietern das Feld „Blocken“ aktiviert?*
  - ☐ ***[Optional]** Ist unter Extras / Internetoptionen / Datenschutz / Erweitert / Cookies von Erstanbietern das Feld „Bestätigen“ aktiviert?*
- ☐ Ist unter dem Menüpunkt *Extras / Internetoptionen / Erweitert* unter „Browsen“ die Option „Sites und Inhalte im Hintergrund laden, um die Leistung zu optimieren“ deaktiviert, um zu verhindern, dass beim Vorabladen von Webseiten private Informationen an Web-Angebote übermittelt werden, die der Benutzer gar nicht öffnen möchte?
- ☐ Ist nur ein Administrator in der Lage, Web-Angebote in eine Zone mit niedrigeren Sicherheitsvorkehrungen zu verschieben (z. B: „Vertrauenswürdige Sites“)?
- ☐ Erfolgt die Verwaltung der Web-Angebote in der Zone „Vertrauenswürdige Sites“ zentral?
- ☐ Wurden die in dieser Checkliste vorgegebenen Einstellungen mit Hilfe von Gruppenrichtlinien konfiguriert, sodass Benutzer die Konfiguration der einzelnen Sicherheitszonen nicht verändern können?
- ☐ **[Optional]** Wurde unter *Extras / Sicherheit* die "Do Not Track" - Anforderungen (nicht nachverfolgen) aktiviert?
- ☐ **[Optional]** Wird unter *Extras / Internetoptionen / Allgemein* als Startseite entweder eine interne Webseite oder about:blank verwendet?
- ☐ **[Optional]** Ist unter dem dem Menüpunkt *Extras / Internetoptionen / Allgemein / Browserverlauf* die Option „Browserverlauf beim Beenden löschen“ aktiviert?
- ☐ **[Optional]** Ist unter dem dem Menüpunkt *Extras / Internetoptionen / Erweitert / Sicherheit* die Option „Beim Wechsel zwischen sicherem und nicht sicherem Modus warnen“ aktiviert?
- ☐ **[Optional]** Ist unter dem dem Menüpunkt *Extras / Internetoptionen / Erweitert / Browsen* die Option „Browsererweiterungen von Drittanbietern aktivieren“ deaktiviert?
- ☐ **[Optional]** Ist unter dem dem Menüpunkt *Extras / Internetoptionen / Erweitert / Multimedia* die Option „Alternative Codecs in HTML5-Medienelementen aktivieren“ deaktiviert?

4.2 Nutzung potenziell gefährlicher Web-Inhalte

Zum Aufbau einer Infrastruktur, mit der auch potenziell gefährliche Inhalte im Web genutzt werden können, existieren mehrere Varianten. Für die Browser-Einstellungen gelten jedoch stets die gleichen Anforderungen, unabhängig davon, ob ein ReCoBS, eine Internet-PC-Zone oder eine virtuelle Surf-Station eingesetzt wird. Der folgende Abschnitt behandelt die Einstellungen, die am Microsoft Internet Explorer zur Nutzung potenziell gefährlicher Web-Inhalte vorgenommen werden müssen.

Terminal-Server und Standard-PCs zur Nutzung potenziell gefährlicher Web-Inhalte

Kommen Terminal-Server oder Standard-PCs zur Nutzung potenziell gefährlicher Web-Inhalte zum Einsatz, gelten in Bezug auf die Sicherheitseinstellungen für Browser sinngemäß die gleichen

Anforderungen wie für interne Clients. Die folgenden Kontrollfragen behandeln lediglich die Abweichungen von der in Abschnitt 4.1 beschriebenen Konfiguration. Der Begriff „Web-System“ bezieht sich dabei sowohl auf Terminal-Server, wenn ReCoBS oder Thin Clients eingesetzt werden, als auch auf Standard-PCs zur Nutzung potenziell gefährlicher Web-Inhalte.

☐ Besteht die Möglichkeit, mit dem Internet Explorer am Web-System Aktive Inhalte wie Java-Script, VBScript und unsignierte Java-Applets zu verwenden?

- ☐ *Sind unter dem Menüpunkt Extras / Internetoptionen / Sicherheit für die Zone „Internet“ die Standardeinstellungen der Sicherheizstufe „Hoch“ ausgewählt?*
- ☐ *Ist unter dem Menüpunkt Extras / Internetoptionen / Sicherheit / Zone „Internet“ / Stufe anpassen / Downloads die Option „Dateidownload“ auf „Aktivieren“ gesetzt?*
- ☐ *Ist unter dem Menüpunkt Extras / Internetoptionen / Sicherheit / Zone „Internet“ / Stufe anpassen / Skripting die Option „Active Scripting“ auf „Aktivieren“ gesetzt?*
- ☐ *Ist unter dem Menüpunkt Extras / Internetoptionen / Sicherheit / Zone „Internet“ / Stufe anpassen / Verschiedenes die Option „*SmartScreen-*Filter verwenden“ auf „Deaktivieren“ gesetzt?*
- ☐ *Ist unter dem Menüpunkt Extras / Internetoptionen / Erweitert unter den Einstellungen „Sicherheit” die Check-Box „SmartScreen-Filter aktivieren“ deaktiviert?*
- ☐ *Sind bei Bedarf Plug-Ins für Flash, MS Silverlight und/oder Java installiert?*

☐ Werden mit Hilfe des Zonenmodells signierte Java-Applets und ActiveX-Controls nur explizit für einzelne Webseiten freigeschaltet?

- ☐ *Sind unter dem Menüpunkt Extras / Internetoptionen / Sicherheit für die Zone „Vertrauens-würdige Sites“ die Standardeinstellungen der Sicherheitsstufe „Mittel bis hoch“ ausgewählt?*
- ☐ *Wurde unter dem Menüpunkt Extras / Internetoptionen / Sicherheit / Zone „Vertrauenswür-dige Sites“ / Stufe anpassen / Verschiedenes die Option „*SmartScreen-*Filter verwenden“ wieder zurück auf „Deaktivieren“ gesetzt?*

☐ Wird die Chronik und der Browser-Cache stets beim Ausloggen der Benutzer gelöscht?

- o Wird im privaten Modus (InPrivate) gearbeitet? (Anmerkung: Durch „iexplore.exe -private“ ist es möglich den Internet Explorer im InPrivate-Modus zu starten) **– oder –**
- o Ist unter dem Menüpunkt *Extras / Internetoptionen / Allgemein / Browserverlauf* die Option „Browserverlauf beim Beenden löschen“ aktiviert?

5 Grundvorgaben für den sicheren Betrieb

Im Betrieb unterscheidet sich der Microsoft Internet Explorer kaum von anderen Browsern. Aus diesem Grund sind lediglich die Anforderungen der allgemeinen Checkliste (ISi-Check zu ISi-Web-Client) zu beachten.

6 Literaturverzeichnis

[ISi-Web-Client] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sichere Nutzung von Web-Angeboten, 2008, https://www.bsi.bund.de/ISi-Reihe

[ITGSK] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT Grundschutzkataloge, Stand 2008, https://www.bsi.bund.de/IT-Gundschutz

[ISi-LANA] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sichere Anbindung lokaler Netze an das Internet, 2014, https://www.bsi.bund.de/ISi-Reihe

[ISi-E] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Einführung, Grundlagen, Vorgehensweise, in Bearbeitung, https://www.bsi.bund.de/ISi-Reihe