

Checkliste IT-Sicherheit

aufgrund eines Beschlusses
des Deutschen Bundestages

IT-Sicherheit in der Produktion		
Gefahr/ Risiko	Erhebung des Ist-Zustands	Maßnahme
Mensch	Fehlende Verantwortlichkeiten und Risikobewusstsein	<p>Sind die Mitarbeiter bezüglich IT-Sicherheit in der Produktion sensibilisiert?</p> <p>Nein →</p> <p>Umgesetzt? </p> <p>Klären Sie Ihre Mitarbeiter über mögliche Sicherheitsrisiken und die Gefahren von Social Engineering auf (vgl. Checkliste Basisschutz). Allen Mitarbeitern sollte bekannt sein, wo und wie sie mit der Produktion verbunden sind und welche Auswirkungen dies hat.</p>
		<p>Sind IT-Sicherheitsleitlinien erstellt worden?</p> <p>Nein →</p> <p>Umgesetzt? </p> <p>Erstellen Sie IT-Sicherheitsleitlinien und weisen Sie auf diese und weitere Vorgaben hin.</p>
		<p>Ist in den Sicherheitsrichtlinien festgeschrieben, wer im Falle eines IT-Notfalls zuständig, beziehungsweise zu benachrichtigen ist (Notfallplan)?</p> <p>Nein →</p> <p>Umgesetzt? </p> <p>Legen Sie einen Verantwortlichen und dessen Entscheidungsbefugnisse fest. Erstellen Sie einen Notfallplan und stellen Sie nach Möglichkeit die Netzwerkgeräte mit einer USV (Unterbrechungsfreie Stromversorgung) aus.</p>
Maschine	Ungewollte interne Zugriffsmöglichkeiten	<p>Ist festgeschrieben, welcher Mitarbeiter worauf zugreifen darf?</p> <p>Nein →</p> <p>Umgesetzt? </p> <p>Legen Sie Zugriffsbeschränkungen fest, wobei nur die Mitarbeiter auf bestimmte Bereiche Zugriff haben sollten, die diesen tatsächlich benötigen. Hinterfragen Sie die Berechtigungen kritisch.</p>
		<p>Werden Updates für Maschinen angeboten und sind diese eingespielt?</p> <p>Nein →</p> <p>Umgesetzt? </p> <p>Die Maschinen sollten nach Möglichkeit mit Updates versorgt werden, wobei Sie diese manuell und nach Rücksprache mit dem Hersteller durchführen sollten. Kann kein Update eingespielt werden (bei Notwendigkeit einer Netzverbindung) darf die Anbindung nur gesichert (DMZ, VLAN etc) erfolgen.</p>
	Fehlende Aktualität der Software	<p>Wenn die Maschine mit einem proprietären Betriebssystem wie Windows ausgerüstet ist, sind Sicherheitsmaßnahmen wie Antivirus und Firewall installiert und eingerichtet (Clientsicherheit)?</p> <p>Nein →</p> <p>Umgesetzt? </p> <p>Lassen es die Ressourcen zu, sollten Sie die Steuerungsrechner mit einer Antivirus-Software ausstatten. Soweit eine Firewall vorhanden ist, sollten Sie diese in jedem Fall nutzen.</p>

Infektion mit Schadsoftware

Ist festgelegt, wer Updates einspielen kann und darf?

Nein

Umgesetzt? 
Legen Sie eine Richtlinie für das Einspielen von Updates und Patches fest (Patchmanagement), in der auch die Zuständigkeiten und Intervalle definiert sind.

Werden Datenträger wie Disketten oder USB-Sticks zum Datenaustausch mit der Maschine und für keinen anderen Zweck verwendet?

Nein

Umgesetzt? 
Achten Sie darauf, dass die externen Datenträger für keine anderen Zwecke gebraucht werden und nur von vertrauenswürdigen Rechnern Daten aufgenommen werden.

Ist das Netzwerk so strukturiert, dass keine Systeme ungewollten Zugriff auf andere erhalten?

Nein

Umgesetzt? 
Trennen Sie die Netze von Produktion und Verwaltung voneinander. Hierfür kommen sowohl Hard- als auch Softwarelösungen in Frage.

Ungewollte externe Zugriffsmöglichkeiten

Sind die Produktionsnetze untereinander getrennt?

Nein

Umgesetzt? 
Separieren Sie die Produktionsnetze bspw. mit Hilfe von VLANs.

Besteht aus dem Produktionsnetz eine Internetverbindung?

Ja

Umgesetzt? 
Prüfen Sie, ob eine Verbindung zum Internet zwingend erforderlich ist. Sofern Maschinen mit dem Internet verbunden sind, sollte dies nur über eine gesicherte Verbindungen wie bspw. VPN möglich sein.

Wurde auf weitere Sicherheitstipps zur Steigerung der IT-Sicherheit hingewiesen?

Nein

 **IT-Sicherheit im Handwerk**
it-sicherheit-handwerk.de

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Task Force „IT-Sicherheit in der Wirtschaft“

Die Task-Force „IT-Sicherheit in der Wirtschaft“ ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task-Force und ihren Angeboten sind unter:

www.it-sicherheit-in-der-wirtschaft.de abrufbar

www.it-sicherheit-handwerk.de



itb- Institut für Technik der Betriebsführung im Deutschen Handwerksinstitut e.V.



Heinz-Piest-Institut für Handwerkstechnik an der Leibniz Universität Hannover



Handwerkskammer Rheinhessen, Kompetenzzentrum für IT-Sicherheit und qualifizierte digitale Signatur



if(is) - Institut für Internet-Sicherheit der Westfälischen Hochschule