We create chemistry

Be Secure Checkliste

zum Informationsschutz als Hilfestellung für Dritte bei der Zusammenarbeit mit der BASF.

Checkliste
zu Informationsschutz und Cybersicherheit

Diese „Checkliste zu Informationsschutz und Cybersicherheit“ soll dem Anwender helfen, potenzielle Gefahrenquellen beim Umgang mit schützenswerten Informationen zu erkennen und entsprechende Maßnahmen und Vorkehrungen zu treffen, damit schützenswerte Informationen jederzeit wirksam gegen Verlust und unberechtigten Zugriff geschützt sind.

Die Erfahrung hat gezeigt, dass die in dieser Checkliste angesprochenen Fragestellungen wesentliche Elemente sind, die bei der praktischen Umsetzung eines jederzeit wirksamen Informationsschutzes eine bedeutende Rolle spielen.

Diese Checkliste hat keinen abschließenden Charakter. Der Anwender hat jeweils eigenverantwortlich zu beurteilen, welche konkreten Maßnahmen und Vorkehrungen zu Informationsschutz und Cybersicherheit im jeweiligen Einzelfall notwendig sind. Dabei sollte sich nie ausschließlich auf technische Lösungen verlassen werden, sondern stets auch gesunder Menschenverstand Anwendung finden.

Impressum:

67056 Ludwigshafen

Informationsschutz und Cybersicherheit
E-Mail: be-secure@basf.com
Stand: Oktober 2019

Grundlegende Fragestellungen

- Ist der Kreis der Personen, die zum Umgang mit schützenswerten Informationen berechtigt sein sollen („Berechtigte"), festgelegt?
- Wurden die Berechtigten ordnungsgemäß zur Vertraulichkeit verpflichtet?
- Wurde den Berechtigten eine Unterweisung zu Informationsschutz und Cybersicherheit erteilt?
- Wird durch regelmäßige Kontrollen geprüft, ob die Vorgaben zum Informationsschutz ordnungsgemäß eingehalten werden?
- Werden Art und Umfang der durchgeführten Maßnahmen zum Informationsschutz nachweisbar dokumentiert?
- Werden im Falle des Umgangs mit personenbezogenen Daten die gesetzlichen Datenschutzbestimmungen eingehalten?
- Werden die Standards bei Software und Hardware eingehalten?

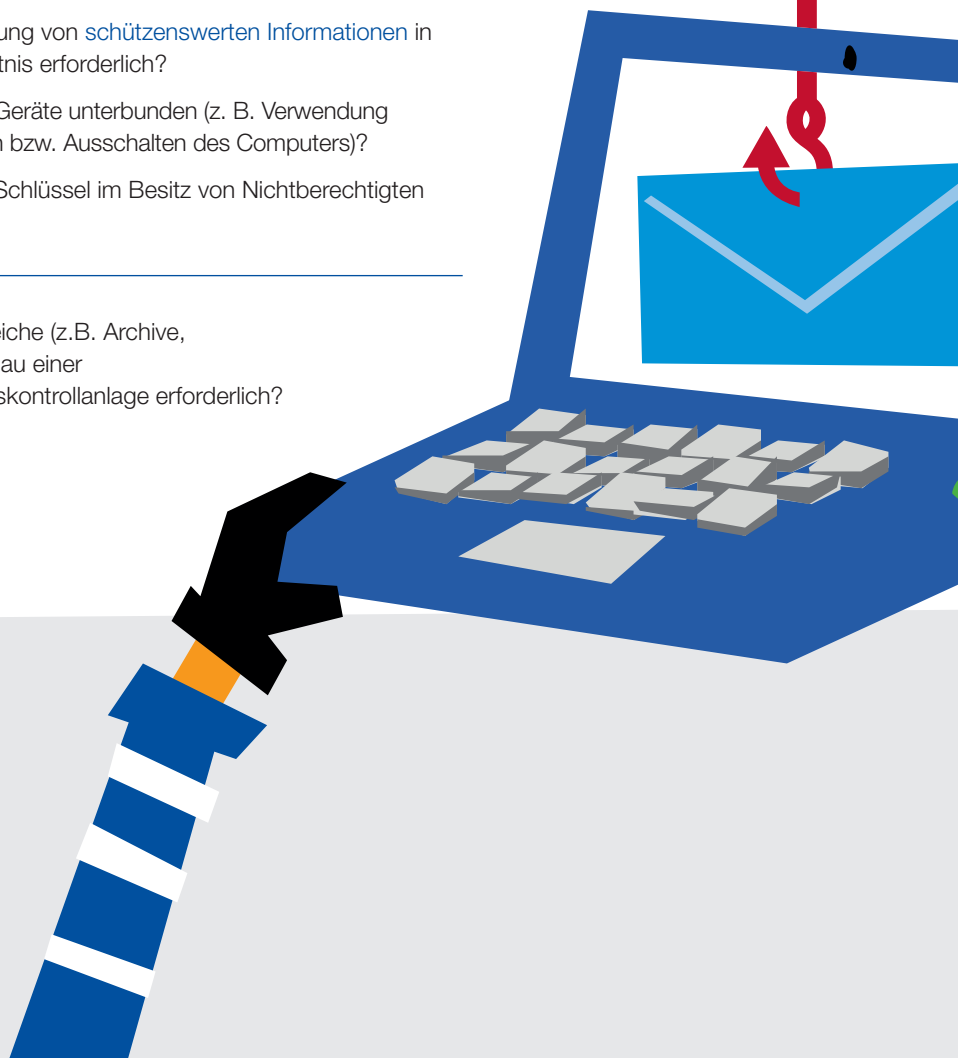
Maßnahmen
gegen unberechtigten Zugriff auf schützenswerte Informationen

Ist der Zugriff auf schützenswerte Informationen jederzeit wirksam auf die Berechtigten beschränkt und werden die Zugriffsrechte in regelmäßigen Abständen überprüft und – soweit erforderlich – angepasst?

Sind bei Abwesenheit des Berechtigten geeignete Schutzmaßnahmen getroffen?

- Ist sichergestellt, dass sich während der Abwesenheit der Berechtigten keine Personen im Raum aufhalten, die zum Umgang mit schützenswerten Informationen nicht berechtigt sind („Nichtberechtigte“)? Findet z.B. die Reinigung von Räumen stets in Anwesenheit des Berechtigten statt?
- Sind Räume, Schränke und sonstige Behältnisse, in denen sich schützenswerte Informationen befinden, bei Abwesenheit des Berechtigten verschlossen?
- Ist möglicherweise die Aufbewahrung von schützenswerten Informationen in einem speziellen Sicherungsbehältnis erforderlich?
- Ist der unberechtigte Zugriff auf IT-Geräte unterbunden (z. B. Verwendung von sicheren Passwörtern, Sperren bzw. Ausschalten des Computers)?
- Ist sichergestellt, dass sich keine Schlüssel im Besitz von Nichtberechtigten befinden?

Ist für besonders schützenswerte Bereiche (z.B. Archive, Serverräume) möglicherweise der Einbau einer Einbruchmeldeanlage und/oder Zutrittskontrollanlage erforderlich?



Maßnahmen
gegen unberechtigten Zugriff auf schützenswerte Informationen

Sichere Passwörter für Systeme, in denen schützenswerte Informationen hinterlegt sind:

- Sind die gewählten Passwörter ausreichend komplex (z.B. sind sie mindestens acht Zeichen lang und enthalten einen Großbuchstaben, einen Kleinbuchstaben, Sonderzeichen und eine Zahl) und werden sie regelmäßig gewechselt?
- Ist sichergestellt, dass Passwörter nicht an Dritte weitergegeben werden und im Falle ihrer Verkörperung (z.B. Niederschrift) nicht frei zugänglich aufbewahrt werden (z.B. Aufbewahrung in einem mit Datum und Unterschrift auf der Verschlusstasche versiegeltem Umschlag in einem Safe)?
- Wird Zwei-Faktor-Authentifizierung verwendet?

Sind hausinterne Postfächer so eingerichtet, dass ein Zugriff von Nichtberechtigten auf im Postfach liegende schützenswerte Informationen nicht möglich ist?

Sind schützenswerte Informationen, die auf Datenträgern (Notebooks, Tablets, Smartphones, Festplatten, Server, CD-ROMs, USB-Sticks, ...) gespeichert sind, wirksam gesichert (z.B. durch Verwendung von Verschlüsselung, die dem Stand der Technik entspricht)?

Werden wirksame Maßnahmen bei der Übermittlung (z.B. E-Mail, Telefon- und Videokonferenzen, Briefversand) von schützenswerte Informationen ergriffen (z.B. Verschlüsselung der Kommunikationsverbindung, Aufteilung der schützenswerte Informationen auf verschiedene Kommunikationsträger)?

Maßnahmen
gegen unberechtigten Zugriff auf schützenswerte Informationen

Sind Drucker und Kopierer sicher konfiguriert? Ist sichergestellt, dass eine Reproduktion von Druck- bzw. Kopieraufträgen, die schützenswerte Informationen enthalten, nicht möglich ist? Wird darauf geachtet, dass Originale, Ausdrucke bzw. Kopien unverzüglich entnommen werden und nicht im Drucker/Kopierer/Faxgerät liegen bleiben (ggf. Verwendung der „PIN-Funktion“)?

- Werden Besprechungen so durchgeführt, dass eine Kenntnisnahme von schützenswerten Informationen durch Nichtberechtigte ausgeschlossen ist?
- Ist sichergestellt, dass Angaben außerhalb des Raumes (z.B. Beschilderung) keinen Rückschluss auf den vertraulichen Inhalt der Besprechung zulassen?
- Ist sichergestellt, dass ein Mithören von außen (z.B. Flur, Nebenräume, Fenster, Türen) nicht möglich ist?
- Ist sichergestellt, dass von außen eine Einsichtnahme in Besprechungs- oder Präsentationsunterlagen ausgeschlossen ist (z.B. Vorhänge schließen)?
- Ist sichergestellt, dass nach Ende der Besprechung keine Unterlagen, Geräte, Präsentationsmedien (Flipchartblätter, Overheadfolien, Whiteboardtexte) zurückgeblieben sind?
- Ist sichergestellt, dass der Besprechungsraum bei allgemeiner Abwesenheit (z.B. in den Pausen) für Nichtberechtigte nicht zugänglich ist?

Qualifizierte Entsorgung
von schützenswerten Informationen

Erfolgt die Entsorgung bzw. Löschung von schützenswerten Informationen qualifiziert und sicher?

- Werden bei der Entsorgung von Papier Cross-Cut-Shredder mit einer maximalen Partikelgröße von 160mm² eingesetzt?
- Beim Einsatz von Sammelbehältern: Sind die Sammelbehälter verschlossen? Sind sie gesichert aufgestellt? Ist der Entsorgungsprozess ausreichend sicher gestaltet? Findet die DIN 66399 (mindestens Sicherheitsstufe 4) Berücksichtigung?

Werden schützenswerte Informationen auf wiederbeschreibbaren elektronischen Datenträgern (z.B. USB-Sticks, Speicherkarten, CD/DVD, Festplatten, ...) vor erneuter Verwendung bzw. vor Weitergabe an Dritte vollständig und sicher gelöscht?

Informationsschutzaspekte auf Reisen und in der Öffentlichkeit

- Wird vor der Reise geprüft, ob die Mitnahme von schützenswerten Informationen tatsächlich zwingend notwendig ist?
- Ist sichergestellt, dass Nichtberechtigte unterwegs keine Einsicht in schützenswerte Informationen (z.B. Akten und Notebook) nehmen können?
- Ist sichergestellt, dass Akten, Notebook, ... unterwegs stets beaufsichtigt sind?
- Ist sichergestellt, dass Nichtberechtigte bei Gesprächen oder Telefonaten nicht mithören können?
- Sind Notebooks mit Hilfe eines geeigneten Schlosses an einer festen Struktur befestigt und so gegen unberechtigte Wegnahme gesichert?
- Ist sichergestellt, dass schützenswerte Informationen nicht auf Internet-Plattformen und sozialen Medien eingestellt sind?
- Ist sichergestellt, dass bei Rückgabe des Miet- oder Leasingfahrzeugs weder Daten (z.B. auf Telefon oder Navigationssystem) gespeichert sind noch Unterlagen zurückgelassen werden?

Persönliche Notizen

Persönliche Notizen

be-secure.basf.net

Stand: Oktober 2019