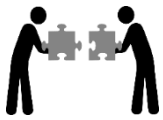
LS03: Incidents priorisieren

Arbeitsaufträge:



☒ Bilden Sie **4-er Teams** mit entsprechender Sitzordnung!

○ **Analysieren** Sie die folgenden Informationen und die **abgebildete ITIL-Prioritätenmatrix (Seiten 2-3).**

○ **Analysieren Sie die folgenden 4 Fälle (Seiten 4-6)** und

notieren bei jedem der Fälle:

➔ die **Dringlichkeit** (niedrig/mittel/hoch)

➔ die **Auswirkung** (niedrig/mittel/hoch)

➔ den **resultierenden Prioritätscode**

Prioritätscodes: 1 = kritisch / 2 = hoch / 3 = mittel / 4 = niedrig / 5 = sehr niedrig

WICHTIG: <u>Begründen Sie ausführlich</u> anhand der genannten Dringlichkeits- und Auswirkungs-Kriterien (z. B. eine minimale Anzahl von Mitarbeitern ist betroffen) Ihre Einschätzung!

○ Informieren Sie sich mithilfe **des Infotextes (Seite 7)** zum Thema **„Major Incidents“**.

Welche/r der 4 Incidents sollte/n aus Ihrer Sicht als Major Incident behandelt werden? Begründen Sie Ihre Antwort!

○ Lassen Sie Ihre **vollständigen Ergebnisse von den Lehrkräften abnehmen**!

Arbeitszeit: 45 min

<u>Abnahme durch Lehrkräfte erfolgt</u>: ○ **Ja** **Kürzel: ……**

○ **Nein, Nachbesserung notwendig bei**

- ○ **Fall 1**
- ○ **Fall 2**
- ○ **Fall 3**
- ○ **Fall 4** **Kürzel: …….**

○ **Abnahme nach Nachbesserung erfolgt**

Kürzel: …….

Definition: Die *Incident-Priorität* ergibt sich in der Regel aus der Bewertung seiner Auswirkung und Dringlichkeit: Dringlichkeit ('Urgency') ist ein Maß dafür, wie schnell der Incident gelöst werden muss. Auswirkung ('Impact') drückt aus, wie umfangreich der Incident ist und welcher (potentielle) Schaden durch den Incident verursacht werden kann.

A: Incident-Dringlichkeit (Dringlichkeits-Kategorien)

Dieser Abschnitt gibt *Incident-Dringlichkeits-Kategorien* vor. Die Definitionen müssen auf die jeweilige Organisation genau abgestimmt sein, deshalb ist die folgenden Tabelle lediglich ein Beispiel:

Um die ***Incident-Dringlichkeit*** zu bestimmen, wähle die höchste zutreffende Kategorie:

Kategorie	Beschreibung
Hoch (H)	• Der von dem Incident verursachte Schaden nimmt im Zeitverlauf schnell zu. • Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind sehr zeitkritisch • Durch schnelles Handeln kann verhindert werden, dass aus einem Minor Incident ein Major Incident wird. • Mehrere Benutzer mit VIP (Very important Persons) –Status sind betroffen.
Mittel (M)	• Der von dem Incident verursachte Schaden nimmt im Verlauf der Zeit substantiell zu. • Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind nur mäßig zeitkritisch. • Ein einzelner Benutzer mit VIP-Status ist betroffen.
Niedrig (N)	• Der von dem Incident verursachte Schaden nimmt im Verlauf der Zeit nur unwesentlich zu. • Die Aufgaben, die von den Mitarbeitern nicht erfüllt werden können, sind nicht zeitkritisch

B: Incident-Auswirkung (Auswirkungs-Kategorien)

Dieser Abschnitt gibt *Incident-Auswirkungs-Kategorien* vor. Die Definitionen müssen auf die jeweilige Organisation genau abgestimmt sein, deshalb ist die folgenden Tabelle lediglich ein Beispiel:

Um die *Incident-Auswirkung* zu bestimmen, wähle die höchste zutreffende Kategorie:

Kategorie	Beschreibung
Hoch (H)	• Eine große Anzahl von Mitarbeitern ist betroffen und/oder kann ihre Aufgaben nicht erfüllen. • Eine große Anzahl von Kunden ist betroffen und/oder ist in irgendeiner Weise akuten Nachteilen ausgesetzt. • Ein finanzieller Schaden durch den Incident ist voraussichtlich höher als (zum Beispiel) 10.000 EUR. • Eine Beschädigung des Ansehens (Reputation) des Unternehmens in großem Umfang ist wahrscheinlich. • Es besteht Gefahr für Leib oder Leben.
Mittel (M)	• Eine mäßige Anzahl von Mitarbeitern ist betroffen und/oder kann ihre Aufgaben nicht erfüllen. • Eine mäßige Anzahl von Kunden ist betroffen und/oder erfährt Einschränkungen beim Komfort. • Ein finanzieller Schaden durch den Incident liegt voraussichtlich zwischen (zum Beispiel) 1.000 EUR und 10.000,00 EUR. • Eine Beschädigung des Ansehens (Reputation) des Unternehmens im mäßigen Umfang ist wahrscheinlich.
Niedrig (N)	• Eine minimale Anzahl von Mitarbeitern ist betroffen und/oder kann ihre Aufgaben erfüllen, jedoch nur mit zusätzlichem Aufwand. • Eine minimale Anzahl von Kunden ist betroffen und/oder erfährt Einschränkungen beim Komfort, jedoch nur in geringem Umfang. • Der finanzielle Schaden durch den Incident ist voraussichtlich weniger als (zum Beispiel) 1.000 EUR. • Die Beschädigung des Ansehens (Reputation) des Unternehmens ist nur in minimalem Umfang zu erwarten.

C: Incident-Priorität (Prioritäts-Kategorien)

Die Priorität eines Incidents leitet sich aus Dringlichkeit und Auswirkung ab.

Incident Priority Matrix

Wenn Klassen zur Bestimmung von Dringlichkeit und Auswirkung definiert sind, kann eine Dringlichkeits-Auswirkungs-Matrix verwendet werden, um Klassen von Prioritäten festzulegen, wie im folgenden Beispiel

		Auswirkung		
		H	M	N
Dringlichkeit	H	1	2	3
	M	2	3	4
	N	3	4	5

Prioritäts-Code	Beschreibung
1	Kritisch
2	Hoch
3	Mittel
4	Niedrig
5	Sehr niedrig

Fall 1:

Ein Mitarbeiter in der Buchhaltung ist total aufgeregt, da er nach dem Runterladen eines Anhanges einer E-Mail Folgendes auf seinem Bildschirm sieht ….

Er teilt Ihnen am Telefon folgendes mit:

„Nach dem Öffnen der E-Mail eines unserer Neukunden aus Litauen, an der eine Auslandsüberweisung als PDF beigefügt war, die ich auch geöffnet habe, steht auf meinem Bildschirm „Your Files are encrypted“, darüber sieht man ein Totenkopfsymbol wie auf einer Piratenflagge – Ich bin ganz verzweifelt, was soll ich denn jetzt machen?“

➔ **Dringlichkeit** (niedrig/mittel/hoch), weil ……

……
der Vorfall ein akutes Sicherheitsproblem darstellt. Ransomware kann sich schnell im U
……

……

……

➔ **Auswirkung** (niedrig/mittel/hoch), weil ……

……
sensible Firmendaten verschlusselt wurden und finanzielle Schaden sowie
……

……

……

➔ R**esultierender Prioritätscode:**

Prioritätscodes: 1 = kritisch / 2 = hoch / 3 = mittel / 4 = niedrig / 5 = sehr niedrig

Fall 2:

Anruf eines Mitarbeiters aus der Marketingabteilung:

„Jedes Mal, wenn ich versuche auf meinem Drucker hier in meinem Büro etwas auszudrucken, erscheint die Meldung „Drucker nicht erkannt“. Nach Rückfragen erfahren Sie, dass der Mitarbeiter die Möglichkeit hat, per USB-Stick die Dokumente im Nachbarbüro auszudrucken.

➔ **Dringlichkeit** (niedrig/mittel/hoch), weil ……

der Mitarbeiter weiterhin Zugriff auf einen funktionierenden Drucker im Nachbarbüro hat. E

➔ **Auswirkung** (niedrig/mittel/hoch), weil ……..

nur ein einzelner Mitarbeiter betroffen ist und die Arbeitsp

➔ **Resultierender Prioritätscode:**

Prioritätscodes: 1 = kritisch / 2 = hoch / 3 = mittel / 4 = niedrig / 5 = sehr niedrig

Fall 3:

Anruf des sehr verärgerten Vertriebsleiters der Autoteile AG:

„Ich bekomme gerade von meinen Mitarbeitern im Außendienst die Nachricht, dass sie seit ca. 20 Minuten mit ihren Notebooks nicht mehr auf die firmeninterne Kundendatenbank zugreifen können und damit auch keine Kundenaufträge mehr anlegen können.“

➔ **Dringlichkeit** (niedrig/mittel/hoch), weil ……

die Außendienstmitarbeiter derzeit nicht auf die Kundendatenbank zugreifen konnen und somit k

➔ **Auswirkung** (niedrig/mittel/hoch), weil ……..

eine große Anzahl von Außendienstmitarbeitern betroffen ist und der Vorfall c

……..

……..

➔ R**esultierender Prioritätscode:**

Prioritätscodes: 1 = kritisch / 2 = hoch / 3 = mittel / 4 = niedrig / 5 = sehr niedrig

Fall 4:

Die 15 Mitarbeiter der Personalabteilung der Autoteile AG, die sich im 3. Stock der Hauptzentrale befindet, bekommen bei einem Druckbefehl jedes Mal die folgende Fehlermeldung „Server ist nicht erreichbar“ und melden sich deswegen per E-Mail beim Service Desk. In zwei Wochen soll aber der Ausdruck von 1.500 Flyern zum Thema „Unfallverhütungsvorschriften“ erfolgen.

➔ **Dringlichkeit** (niedrig/mittel/hoch), weil

……

der Druck aktuell nicht dringend benötigt wird, der Vorfall aber spätestens in zwei W

……

……

……

……

➔ **Auswirkung** (niedrig/mittel/hoch), weil ……

……

15 Mitarbeiter betroffen sind und die Arbeitsfähigkeit eingeschränkt ist. Der Vorfall kos

……

……

➔ R**esultierender Prioritätscode:**

Prioritätscodes: 1 = kritisch / 2 = hoch / 3 = mittel / 4 = niedrig / 5 = sehr niedrig

D: Kriterien für die Behandlung eines Incidents als Major Incident

Indikatoren:

Über das oben gezeigte Schema hinaus ist es oft angeraten, zusätzliche und leicht verständliche Indikatoren zur Bestimmung von Major Incidents zu definieren.

Beispiele für solche Indikatoren sind:

1. Bestimmte (Gruppen von) geschäftskritischen Services, Anwendungen oder Infrastruktur-Komponenten sind nicht verfügbar und die voraussichtliche Zeit bis zur Wiederherstellung ist zu lang oder unbekannt
2. Bestimmte (Gruppen von) geschäftskritischen Prozessen ("Vital Business Functions") sind betroffen und die voraussichtliche Zeit bis zur Wiederherstellung der vollständigen Leistungsfähigkeit dieser Prozesse ist übermäßig lang oder unbekannt

Die wichtigsten Eigenschaften von Major Incidents

Die wichtigsten Eigenschaften, an denen sich Major Incidents erkennen lassen, sind unter anderem:

- Eine signifikante Anzahl von Kunden bzw. von wichtigen Kundengruppen ist betroffen.
- Die Kosten bzw. aus dem Incident resultierenden Verluste für Kunden und/oder die Service-Organisation sind beträchtlich.
- Die Reputation des Service-Providers wird wahrscheinlich beschädigt.

UND

- Der Arbeits- und Zeitaufwand zur Lösung des Incidents ist vermutlich groß und es ist sehr wahrscheinlich, dass bestehende Service-Level-Vereinbarungen verletzt werden.

Ein Major Incident ist in aller Regel auch mit der Priorität "Kritisch" oder "Hoch" versehen.

Zu beachten ist auch, dass unkritische Incidents durch Fehler oder zu lange Inaktivität zu Major Incidents werden können.

Welche/r der 4 Incidents sollte/n aus Ihrer Sicht als Major Incident behandelt werden? Begründen Sie Ihre Antwort!

Fall 1 und Fall 3 sollten als Major Incidents behandelt werden.

Begrundung:Fall 1 (Ransomware): Der Vorfall stellt eine erhebliche Bedrohung fur die IT-Sic

Quelle: Checkliste Incident-Priorität | IT Process Wiki (it-processmaps.com)