प्रयोगशाला कार्य – 2

1. जोखिम: आवश्यकताओं की स्पष्टता का अभाव:

* विवरण: उपयोगकर्ता खातों (नौकरी चाहने वालों, नियोक्ताओं) के लिए आवश्यकताओं को निर्धारित करने के लिए एक स्पष्ट तंत्र का अभाव, जिससे पंजीकरण और प्रमाणीकरण प्रक्रिया में समस्याएं हो सकती हैं।
* महत्त्व: 4 (उपयोग के प्रारंभिक चरण में समस्याओं को रोकने के लिए महत्वपूर्ण)
* कठिनाई: 3 (दस्तावेज़ीकरण में अधिक स्पष्टता की आवश्यकता है)
* शमन रणनीति के तरीके:

1. प्रत्येक प्रकार के उपयोगकर्ता के लिए विस्तृत पंजीकरण परिदृश्य विकसित करें।
2. संभावित मुद्दों की पहचान करने के लिए उपयोगकर्ताओं के साथ नामांकन परिदृश्यों का परीक्षण करें।

* माना जाता है: हाँ।

1. जोखिम: अनुचित निर्भरता प्रबंधन।

* विवरण: सिस्टम के विभिन्न घटकों के बीच एकीकरण का अभाव, जैसे कि नौकरी खोज प्रणाली और आवेदन प्रक्रिया के बीच, जिससे अप्रत्याशित त्रुटियां हो सकती हैं।
* महत्त्व: 4 (सिस्टम के सुसंगत और प्रभावी कामकाज को सुनिश्चित करने के लिए महत्वपूर्ण)
* कठिनाई: 3 (निर्भरता की अधिक गहन परिभाषा की आवश्यकता है)
* शमन रणनीति के तरीके:

1. सिस्टम के विभिन्न घटकों के बीच स्पष्ट इंटरफेस का विकास।
2. प्रक्रियाओं का नियमित परीक्षण जो एक दूसरे पर निर्भर करते हैं।

* माना जाता है: हाँ।

1. जोखिम: अप्रभावी प्रौद्योगिकी प्रबंधन।

* विवरण: भुगतान प्रणालियों के संचालन में संभावित समस्याएं या मोबाइल एप्लिकेशन में त्रुटियां विफलताओं का कारण बन सकती हैं जो सिस्टम की उपयोगिता को प्रभावित करती हैं।
* महत्त्व: 4 (अपटाइम के लिए महत्वपूर्ण)
* कठिनाई: 3 (अधिक गहन परीक्षण और अद्यतन की आवश्यकता है)
* शमन रणनीति के तरीके:

1. एक निगरानी प्रणाली का कार्यान्वयन और तकनीकी तत्वों का आवधिक अद्यतन।
2. प्रौद्योगिकी का उपयोग करने के सुरक्षित और प्रभावी तरीकों पर कर्मियों के प्रशिक्षण का संचालन करना।

* माना जाता है: हाँ।

1. जोखिम: खराब सुरक्षा।

* विवरण: विश्वसनीय सुरक्षा की कमी सिस्टम को SQL इंजेक्शन, XSS और अन्य जैसे वेब हमलों के प्रति संवेदनशील बनाती है, जिससे गोपनीय जानकारी का रिसाव हो सकता है और उपयोगकर्ता का विश्वास कम हो सकता है।
* महत्त्व: 5 (असुरक्षित प्रथाओं के रूप में महत्वपूर्ण गोपनीय जानकारी के रिसाव और उपयोगकर्ता विश्वास के नुकसान का कारण बन सकता है)
* कठिनाई: 4 (उच्च तकनीकी विशेषज्ञता और अतिरिक्त सुरक्षा उपकरणों के कार्यान्वयन की आवश्यकता है)
* शमन रणनीति के तरीके:

1. दुर्भावनापूर्ण ट्रैफ़िक को फ़िल्टर करने और हमलों को रोकने के लिए एक मजबूत वेब एप्लिकेशन फ़ायरवॉल (WAF) लागू करें।
2. संभावित कमजोरियों की पहचान करने और उन्हें ठीक करने के लिए एप्लिकेशन कोड को नियमित रूप से अपडेट और ऑडिट करें।
3. सुरक्षित विकास प्रथाओं पर कर्मचारियों को प्रशिक्षित करें और सुरक्षा मानकों का अनुपालन सुनिश्चित करें।

* माना जाता है: हाँ।

1. जोखिम: उपयोगकर्ता के पंजीकरण करने पर पुष्टिकरण ईमेल भेजने में विफलता।

* विवरण: पंजीकरण के दौरान एक तुच्छ सर्वर गड़बड़ के मामले में, उपयोगकर्ता को मेल की पुष्टि प्राप्त नहीं हो सकती है, जो संभावित उपयोगकर्ता को खोने और विश्वास खोने का जोखिम पैदा करता है।
* गंभीरता: 5 (महत्वपूर्ण, छूटे हुए उपयोगकर्ता, और विश्वास की हानि)।
* कठिनाई: 2 (तकनीकी समस्या)।
* शमन रणनीति के तरीके:

1. अधिक उत्पादक और स्थिर लोगों के साथ सर्वरों का प्रतिस्थापन।
2. लिखित पुष्टि के लिए अनुरोध पुनः सबमिट करने की क्षमता।

* माना जाता है: हाँ।

1. जोखिम: प्लेटफ़ॉर्म प्रशासकों और हेल्प डेस्क की कमी।

* विवरण: परियोजना निश्चित रूप से किसी दिन बहुत सारे ट्रैफ़िक की सेवा करेगी, इसे नियंत्रित करने के लिए, एक बड़े कर्मचारियों को बनाए रखने से एक युवा कंपनी के लिए एक बहुत पैसा खर्च हो सकता है।
* महत्त्व: 4 (पार्टियों के हितधारकों की धारणा के दृष्टिकोण से बहुत महत्वपूर्ण)।
* कठिनाई: 3 (एक विश्वसनीय सीआरएम सेवा प्रदाता ढूंढना)।
* शमन रणनीति के तरीके:

1. कर्मचारियों की जरूरतों की भविष्यवाणी करने के लिए यातायात निगरानी।
2. एक विश्वसनीय सीआरएम सेवा प्रदाता के साथ दीर्घकालिक साझेदारी स्थापित करना।
3. एक कृत्रिम बुद्धिमत्ता बॉट के माध्यम से नियमित कार्यों का स्वचालन।

* माना जाता है: हाँ।

1. जोखिम: उपयोगकर्ता अपनी व्यक्तिगत प्रोफ़ाइल का दुरुपयोग करते हैं और फ़िशिंग लिंक पोस्ट करते हैं।

* विवरण: उपयोगकर्ता फ़िशिंग लिंक पोस्ट करके अपनी प्रोफ़ाइल का दुरुपयोग कर सकते हैं, जो सीधे उपयोगकर्ताओं के डेटा और उपकरणों की सुरक्षा को प्रभावित करता है।
* गंभीरता: 5 (अत्यंत महत्वपूर्ण, डेटा और उपकरणों की सुरक्षा को प्रभावित करता है)।
* कठिनाई: 2 (तकनीकी भाग से समाधान)।
* शमन रणनीति के तरीके:

1. हर बार जब आप सेवा में लॉग इन करते हैं, तो उपयोगकर्ता को याद दिलाएं कि उन्हें अपनी आँखें खुली रखने और उन्हें संभावित शुभचिंतकों की याद दिलाने की आवश्यकता है।
2. सीआरएम प्रणाली के माध्यम से प्रकाशन से पहले लिंक की जांच करने की क्षमता।

* माना जाता है: हाँ।

1. जोखिम: प्लेटफ़ॉर्म व्यवस्थापक को संदेशों/अनुरोधों के बीच गड़बड़।

* सारांश: विभिन्न अनुरोधों में भ्रम प्रसंस्करण और प्रतिक्रियाओं को धीमा कर सकता है, जिससे सेवा की जवाबदेही प्रभावित होती है।
* महत्व: 4 (सेवा की जवाबदेही को प्रभावित करता है)।
* कठिनाई: 1 (हल करने में आसान)।
* शमन रणनीति के तरीके:

1. संदेशों की सक्षम छँटाई के लिए टेम्पलेट थीम जोड़ना।
2. तत्काल आवश्यकता के मामले में वर्तमान व्यवस्थापक को पुनर्निर्देशित करें।

* माना जाता है: हाँ।

1. जोखिम: त्रुटि प्रबंधन।

* सारांश: त्रुटियां होने पर भ्रम समस्या निवारण प्रक्रिया को धीमा कर सकता है।
* महत्त्व: 4 (त्रुटि समाधान की गति को प्रभावित करता है)
* कठिनाई: 2 (समय में समस्याओं की पहचान करने में कठिनाई)
* शमन रणनीति के तरीके:

1. सरल भाषा में सूचनात्मक त्रुटि संदेश बनाना महत्वपूर्ण है।
2. एक त्रुटि लॉग लागू करें जो अधिक कुशल समस्या निवारण के लिए त्रुटि की उत्पत्ति और कारण का रिकॉर्ड रखेगा।
3. ऐसे व्यक्तियों को नियुक्त करें जो समय-समय पर सिस्टम के विभिन्न पहलुओं का परीक्षण करेंगे और डेटा एकत्र करेंगे।

* माना जाता है: हाँ।