FACH HOCHSCHULE LÜBECK
University of Applied Sciences

Methodisch-didaktisches Konzept - pMOOC

Name des Kurses: Netzwerksicherheit

Struktur

AUFSTIEG DURCH BILDUNG >> OFFENE HOCHSCHULEN

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

FACH HOCHSCHULE LÜBECK
University of Applied Sciences

A Rahmenbedingungen Ihres pMOOCs

Name des MOOCs: Netzwerksicherheit (Hashtag #nwsMOOC)

Autoren: Andreas Hanemann, Wolfgang Hommel, Helmut Reiser (basierend auf dem MI-Online-Master Modul „Sicherheitstechniken in Kommunikationsnetzen“)

Kursformat: xMOOC

Kurzvorstellung des MOOCs: (Führen Sie hier in 3-4 Sätzen aus, worum es bei Ihrem Kurs geht)
In diesem MOOC geht es um aktuelle Themen der Netzwerksicherheit, die mittels Texten, Animationen und Videos vermittelt werden. Dabei werden Angriffsmöglichkeiten auf Rechnernetze, Schutzmaßnahmen und sichere Kommunikationsmöglichkeiten über das Internet vorgestellt. Ergänzend zu den technischen Fragenstellungen wird erläutert, welchen Nutzen die Standards IT-Grundschutz und ISO/IEC 27000 für die Informationssicherheit von Organisationen bieten.

Hier ein Vorschlag für eine „werbendere“ Version für die MOOC-Plattform:

In den letzten Jahren wurden vielfach gravierende Probleme bei der Netzwerksicherheit bekannt, die erhebliche finanzielle Auswirkungen auf die betroffenen Firmen hatten. Daher herrscht in vielen Organisationen Unsicherheit darüber, ob die eigenen Maßnahmen zur Netzwerksicherheit (z.B. Firewalls, Virenscanner, Mitarbeiterschulungen) ausreichend sind. Dieser MOOC möchte ein umfassendes und praxisnahes Bild der heutigen Situation darstellen, inklusive Angriffsszenarien, Abwehrmaßnahmen sowie Möglichkeiten der sicheren Kommunikation. Teilnehmer des MOOCs werden anschließend die Situation in der eigenen Organisation besser beurteilen sowie Maßnahmen zu Verbesserung anregen können.

An welche Zielgruppe richtet sich der Kurs in erster Linie?

ExpertInnen (Kenntnisse über Netzwerke auf Bachelorniveau, berufliche Tätigkeit mit Bezug zum Netz der eigenen Organisation)

Welche Kenntnisse und Fertigkeiten setzen Sie bei Teilnehmenden voraus, die Ihren Kurs belegen?

Kenntnisse zur Funktionsweise von Rechnernetzen und dem Internet (z.B. durch das Modul „Kommunikationsnetze I“ aus dem MI-Online Bachelor)

FACH HOCHSCHULE LÜBECK
University of Applied Sciences

B Lernergebnisse Ihres pMOOCs

Lernergebnis 1:

Die TeilnehmerInnen können die Relevanz von aktuellen und zukünftigen Angriffsszenarien auf Rechnernetze aus der Sicht einer Organisation einschätzen. Sie können außerdem vorgestellte Tools anwenden, um selbstständig einfache Sicherheitsuntersuchungen durchzuführen.

Lernergebnis 2:

Die TeilnehmerInnen können für eine Organisation eine angemessene Lösung zum Schutz vor Angriffen aus dem Internet ausarbeiten. Angemessen bedeutet hier, dass diese Lösung eine geeignete Abwägung zwischen dem Nutzen durch die Abwehr möglicher Gefahren und dem Aufwand für die Durchführung der Schutzmaßnahmen darstellt.

Lernergebnis 3:

Die TeilnehmerInnen können für eine Organisation, deren MitarbeiterInnen über das Internet miteinander kommunizieren, eine existierende Lösung hinsichtlich der Sicherheitsaspekte (inklusive von Verfügbarkeitsaspekten) bewerten und alternative Lösungen unter Verwendung von bekannten Protokollen entwerfen.

Lernergebnis 4:

Die TeilnehmerInnen können evaluieren, ob eine Organisation von den internen Strukturen und Vorgehensweise her gut auf Risiken für die Informationssicherheit eingestellt ist. Hierzu können die TeilnehmerInnen standardisierte Rahmenwerke für die Analyse einsetzen.

FACH HOCHSCHULE LÜBECK
University of Applied Sciences

C Lernergebnisse und Lernaktivitäten Ihres pMOOCs

Nachdem Sie nun einige Informationen zu dem Zusammenspiel von Lernergebnissen und Lernaktivitäten erfahren haben, möchten wir Sie bitten, folgende Tabelle auszufüllen, die dies für Ihren Kurs abbildet:

Lernergebnis	Mit folgenden Lernaktivitäten ist das Erreichen des Lernergebnisses überprüfbar
Lernergebnis 1	Multiple-Choice-Fragen müssen beantwortet werden. Um die richtigen Antworten geben zu können, müssen entweder Texte durchgelesen oder Animationen/Videos angesehen werden. Die erfolgreiche Verwendung von Tools wird dadurch überprüft, dass gewisse Testergebnisse mitgeteilt werden müssen (z.B. Nummern, die automatisch prüfbar sind).
Lernergebnis 2	Multiple-Choice-Fragen müssen beantwortet werden. Um die richtigen Antworten geben zu können, müssen entweder Texte durchgelesen oder Animationen/Videos angesehen werden.
Lernergebnis 3	Multiple-Choice-Fragen müssen beantwortet werden. Um die richtigen Antworten geben zu können, müssen entweder Texte durchgelesen oder Animationen/Videos angesehen werden. Die erfolgreiche Verwendung von Tools wird dadurch überprüft, dass gewisse Testergebnisse mitgeteilt werden müssen (z.B. Parameter, die automatisch prüfbar sind).
Lernergebnis 4	Multiple-Choice-Fragen müssen beantwortet werden. Um die richtigen Antworten geben zu können, müssen entweder Texte durchgelesen oder Videos angesehen werden.

FACH HOCHSCHULE LÜBECK
University of Applied Sciences

D Struktur Ihres pMOOCs

Thema 1: Einführung **Laufzeit: 1 Woche** **Woche 1**
Inhaltliche Gliederung des Themas und Darstellungsform(en) (nur zentrale Inhalte) Willkommensvideo; Einführungstext zur Bedeutung des Themas „Netzwerksicherheit“; Gelegenheit zur Wiederholung des OSI-Modells (Text im LOOP und Videos; beim Video ggf. inklusive Kontrollfragen)
Auf welche Lernergebnisse nehmen die Inhalte Bezug? (siehe oben) Es handelt sich um eine Einführung. Es geht noch nicht um die eigentlichen Lernergebnisse, aber man kann das Vorwissen zum OSI-Modell überprüfen.
Welche Lehraktivitäten wollen Sie in diesem Themenkomplex einsetzen bzw. welche Lernaktivitäten wollen Sie initiieren? Die TeilnehmerInnen sollen die Texte und Videos durchlesen bzw. ansehen.
Welche Aufgabenstellungen sollen die Studierenden bearbeiten? (in welcher Sozialform?) Multiple-Choice-Fragen zum OSI-Modell können bearbeitet werden.
Ist ggf. für das Thema ein Leistungsnachweis vorgesehen? Wenn ja, welcher Art? Welches Lernergebnis (s.o.) soll damit nachgewiesen werden? nein

FACH HOCHSCHULE LÜBECK
University of Applied Sciences

Thema 2: Angriffe aus dem Internet
Laufzeit: 3 Wochen
Woche 2–4

Inhaltliche Gliederung des Themas und Darstellungsform(en) (nur zentrale Inhalte)

In sechs Lektionen werden im LOOP Angriffsmöglichkeiten auf Rechnernetze dargestellt, wobei das OSI-Modell zur Gliederung dient (Details siehe Excel-Datei); die Inhalte werden als Texte angeboten, wobei wichtige Zusammenhänge zusätzlich als Videos dargestellt werden

Auch wenn das Lernmodul mehrere Wochen dauert, sollen dessen Inhalte auf einmal freigeschaltet werden.

Auf welche Lernergebnisse nehmen die Inhalte Bezug? (siehe oben)

Lernergebnis 1

Welche Lehraktivitäten wollen Sie in diesem Themenkomplex einsetzen bzw. welche Lernaktivitäten wollen Sie initiieren?

Die TeilnehmerInnen sollen die Texte und Videos durchlesen bzw. ansehen. Außerdem sollen Untersuchungen mit Angriffswerkzeugen durchgeführt werden.

Welche Aufgabenstellungen sollen die Studierenden bearbeiten? (in welcher Sozialform?)

Multiple-Choice-Aufgaben soll jeder für sich machen. Für die Verwendung der Angriffswerkzeuge kann ein Forum eingerichtet werden, so dass sich die TeilnehmerInnen austauschen können.

Ist ggf. für das Thema ein Leistungsnachweis vorgesehen? Wenn ja, welcher Art? Welches Lernergebnis (s.o.) soll damit nachgewiesen werden?

Die Multiple-Choice-Aufgaben müssen (größtenteils) richtig beantwortet sein. Ein Badge „White Hat Hacker“ wird vergeben, wenn Aufgaben mit praktischen Tools zusätzlich gelöst werden.

FACH HOCHSCHULE LÜBECK
University of Applied Sciences

Thema 3: Abwehr von Angriffen
Laufzeit: 3 Wochen
Woche 5–7

Inhaltliche Gliederung des Themas und Darstellungsform(en) (nur zentrale Inhalte)

In sechs Lektionen werden im LOOP Schutzmechanismen für Rechnernetze dargestellt, wobei das OSI-Modell zur Gliederung dient (Details siehe Excel-Datei); die Inhalte werden als Texte angeboten, wobei wichtige Zusammenhänge zusätzlich als Videos dargestellt werden.

Auch wenn das Lernmodul mehrere Wochen dauert, sollen dessen Inhalte auf einmal freigeschaltet werden.

Auf welche Lernergebnisse nehmen die Inhalte Bezug? (siehe oben)

Lernergebnis 2

Welche Lehraktivitäten wollen Sie in diesem Themenkomplex einsetzen bzw. welche Lernaktivitäten wollen Sie initiieren?

Die TeilnehmerInnen sollen die Texte und Videos durchlesen bzw. ansehen.

Welche Aufgabenstellungen sollen die Studierenden bearbeiten? (in welcher Sozialform?)

Multiple-Choice-Aufgaben soll jeder für sich machen. Außerdem sollen Browser AddOns ausprobiert werden und über deren Nützlichkeit soll abgestimmt sowie diskutiert werden.

Ist ggf. für das Thema ein Leistungsnachweis vorgesehen? Wenn ja, welcher Art? Welches Lernergebnis (s.o.) soll damit nachgewiesen werden?

Die Multiple-Choice-Aufgaben müssen (größtenteils) richtig beantwortet sein. Ein Badge „Secure Browsing“ wird bei Beteiligung an Abstimmungen zu Browser AddOns vergeben.

FACH HOCHSCHULE LÜBECK
University of Applied Sciences

Thema 4: Sicherheitsprotokolle
Laufzeit: 3 Wochen
Woche 8–10

Inhaltliche Gliederung des Themas und Darstellungsform(en) (nur zentrale Inhalte)

In sechs Lektionen werden im LOOP Möglichkeiten zur sicheren Kommunikation über das (unsichere) Internet dargestellt, wobei das OSI-Modell zur Gliederung dient (Details siehe Excel-Datei); die Inhalte werden als Texte angeboten, wobei wichtige Zusammenhänge zusätzlich als Videos dargestellt werden.

Auch wenn das Lernmodul mehrere Wochen dauert, sollen dessen Inhalte auf einmal freigeschaltet werden.

Auf welche Lernergebnisse nehmen die Inhalte Bezug? (siehe oben)

Lernergebnis 3

Welche Lehraktivitäten wollen Sie in diesem Themenkomplex einsetzen bzw. welche Lernaktivitäten wollen Sie initiieren?

Die TeilnehmerInnen sollen die Texte und Videos durchlesen bzw. ansehen. Außerdem sollen Untersuchungen mit Werkzeugen zur sicheren Kommunikation durchgeführt werden.

Welche Aufgabenstellungen sollen die Studierenden bearbeiten? (in welcher Sozialform?)

Multiple-Choice-Aufgaben soll jeder für sich machen. Für die Verwendung der Kommunikationstools kann ein Forum eingerichtet werden, so dass sich die TeilnehmerInnen austauschen können.

Ist ggf. für das Thema ein Leistungsnachweis vorgesehen? Wenn ja, welcher Art? Welches Lernergebnis (s.o.) soll damit nachgewiesen werden?

Die Multiple-Choice-Aufgaben müssen (größtenteils) richtig beantwortet sein. Ein Badge „Secure Communicator“ wird vergeben, wenn Aufgaben mit praktischen Tools zusätzlich gelöst werden.

FACH HOCHSCHULE LÜBECK
University of Applied Sciences

Thema 5: IT-Grundschutz und ISO 27000

Laufzeit: 2 Wochen
Woche 11-12

Inhaltliche Gliederung des Themas und Darstellungsform(en) (nur zentrale Inhalte)

Die Gliederung erfolgt in die Lektionen „IT-Sicherheitsprozesse“, „IT-Grundschutz“, „ISO 27000“ und „Weitere Standards“; die Inhalte werden als Texte im LOOP angeboten, wobei wichtige Zusammenhänge zusätzlich als Videos dargestellt werden

Auf welche Lernergebnisse nehmen die Inhalte Bezug? (siehe oben)

Lernergebnis 4

Welche Lehraktivitäten wollen Sie in diesem Themenkomplex einsetzen bzw. welche Lernaktivitäten wollen Sie initiieren?

Die TeilnehmerInnen sollen die Texte und Videos durchlesen bzw. ansehen.

Welche Aufgabenstellungen sollen die Studierenden bearbeiten? (in welcher Sozialform?)

Multiple-Choice-Aufgaben soll jeder für sich machen.

Ist ggf. für das Thema ein Leistungsnachweis vorgesehen? Wenn ja, welcher Art? Welches Lernergebnis (s.o.) soll damit nachgewiesen werden?

Die Multiple-Choice-Aufgaben müssen (größtenteils) richtig beantwortet sein. Ein Badge „Security Manager“ wird vergeben, wenn Aufgaben mit praktischen Tools zusätzlich gelöst werden.

FACH HOCHSCHULE LÜBECK
University of Applied Sciences

E Literaturliste

Bitte geben Sie hier Ihre verwendete/ empfohlene Literatur an:

- Michael Brenner, Nils Otto vor dem gentschen Felde, Wolfgang Hommel, Helmut Reiser und Thomas Schaaf: "Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung", Hanser Verlag, München, 2011.
- Wolfgang Böhmer: "VPN - Virtual Private Networks - Die reale Welt der virtuellen Netze", Hanser Verlag, München, 2002.
- Claudia Eckert: "IT-Sicherheit, Konzepte - Verfahren - Protokolle", 8. Auflage, Oldenburg Verlag, 2013.
- iX Kompakt Security, 4/2014, Heise Zeitschriften Verlag, Hannover, 2014.
- Heinrich Kersten, Jürgen Reuter, Klaus-Werner Schröder: IT-Sicherheitsmanagement nach ISO27001 und Grundschutz - Der Weg zur Zertifizierung, 4. Auflage, Springer Vieweg, Wiesbaden, 2013.
- James F. Kurose und Keith W. Ross: "Computernetzwerke - Der Top-Down-Ansatz", 6. Auflage, Pearson Studium, München, 2014.
- Jörg Rech: "Wireless LANs", 4. Auflage, Heise Zeitschriften Verlag, 2012.
- Klaus Schmeh: "Kryptographie. Verfahren, Protokolle, Infrastrukturen", d.punkt Verlag, Heidelberg, 2013.
- William Stallings: "Network Security Essentials - Applications and Standards", Fifth Edition, Pearson, Harlow, England, 2014.
- Andrew S. Tanenbaum und David J. Wetherall: "Computernetzwerke", 5. Auflage, Pearson Studium, München, 2012.