

Die US-CCU Cybersicherheitskontroll- liste

von

John Bumgarner und Scott Borg

2007

Übersetzt von Tamara Black and Billie Black
IBM



© 2006-2007 U.S. Cyber Consequences Unit

Diese Cybersicherheitskontrollliste wird umsonst bereitgestellt, die ist aber rechtlich geschützt, und darf nicht verkauft werden oder in anderer Form wiederverkauft werden ohne die ausdrückliche Erlaubnis der U.S. Cyber Konsequenzen Abteilung, ein gemeinnütziges Forschungsinstitut.

Diejenigen, die diese Liste verwenden, sollten bemerken, daß keine Cybersicherheitskontrollliste völlig fehlerlos ist, und dass die in dieser Kontrollliste aufgezählten Verteidigungsmaßnahmen im Prinzip übergangen werden könnten. Die US Cyber Konsequenzen Abteilung kann nicht verantwortlich gehalten werden für Folgen die von der Ausführung der Liste stemmen noch für irgendwelche Fehler die vielleicht in dieser Liste enthalten sind..

Es ist die Absicht der US Cyber Konsequenzen Abteilung diese Kontrollliste jährlich zu aktualisieren. Vorschläge für Verbesserungen sind sehr willkommen und können zu dieser Adresse geschickt werden: checklist_comments@usccu.us

Zu denjenigen, die Vorschläge nach der Begutachtung einer früheren Abfassung angeboten haben, sind die Autoren sehr dankbar.

DIE U.S.–C.C.U. CYBERSICHERHEITSKONTROLL-LISTE

JOHN BUMGARNER UND SCOTT BORG

Diese Kontrollliste ist als ein umfassender Überblick über die Schritte beabsichtigt, die Vereinigungen und andere Organisationen nehmen sollten, um ihre Verwundbarkeit von Cyberangriffen zu reduzieren. Die Grundlage für diese Liste ist die große Zahl von wirklichen Cybersicherheitsanfälligkeiten die im Laufe der Arbeit von John Bumgarner, der Forschungsdirektor für die Sicherheitstechnologie in der US Cyber Konsequenzen Abteilung, und Scott Borg, der Direktor der US Cyber Konsequenzen Abteilung, entdeckt wurden. Es war nur, nachdem diese Liste begann sich der jetzigen Länge zu nähern, dass die Autoren vorherige Cybersicherheitskontroll-Listen untersucht haben um sicherzustellen, daß alle wichtigen Themen in der jetzigen Verfassung enthalten sind. Vorentwürfe der neuen Kontrollliste wurden dann unter einer großen Anzahl von Cybersicherheitsfachleuten in Umlauf gesetzt, und hunderte von Anmerkungen wurden gesammelt. Mit der Integrierung aller praktischeren Vorschlägen die sich in ein umfassendes Dokument entwickelt haben, haben die Autoren versucht einen ziemlich vollständigen Plan für die vorhandenen Cyberangriffe und die Schutzmaßnahmen herzustellen.

Um die Organisation der Kontrollliste als klar und intuitiv als möglich zu machen, wurden die Verwundbarkeiten und Gegenmaßnahmen gemäß sechs einfach zu unterscheidenden Kategorien für Informationssystemelementen sortiert. 1) Hardware, 2) Software, 3) Verkettete Netze, 4) Automatisierung 5) Menschen, und 6) Lieferanten.

Einige weitere Punkte sollten es mehr verständlich machen wie diese Kategorien angewendet werden. Softwareverwundbarkeiten sind wirklich Softwarezugangsverwundbarkeiten, nachdem die Software produziert, nachgeprüft, und installiert worden ist, muß dann jemand Zugang haben um eine Sicherheitsgefahr zu bekommen. Softwarelieferungsverwundbarkeiten müssen als ein Bestandteil der Informationssystemverwundbarkeiten behandelt werden, da Softwarelieferanten regelmässig mit Informationssystemen aufeinander wirken lange nach dem anfänglichen Verkauf oder der Software lizenzierung. Andere Typen von Lieferanten brauchen im allgemeinen nicht als Informationssystemverwundbarkeiten behandelt zu werden, da sie nicht wirklich laufende Teilnehmer in den Informationssystem Operationen sind.

Automationsverwundbarkeiten umfassen nicht nur alle Systeme, die zwischen Informationsprozessen und physischen Prozessen vermitteln, sondern auch alle automatischen Prozesse die physische Produkte erzeugen. Da praktisch jedes Informationssystem mindestens ein physisches Produkt erzeugt - seine eigenen Sicherheitsmedien- Automationsverwundbarkeiten sind nicht nur wichtig für physische Industrien, sondern für alle Informationssystemen.

Diese Hauptgebiete, in denen Cyberangriffe stattfinden könnten, ist weiter in zwei oder mehr Angriffsalleen unterteilt worden. Diese engeren Angriffsalleen werden gemäß den Tätigkeiten die ausgeführt oder beaufsichtigt werden müssen organisiert, um die Sicherheit jener Informationssystembestandteile aufrechtzuerhalten. Das führt zu sechzehn Alleien, organisiert gemäß der folgenden Tabelle.

ÜBERSICHT VON HAUPTCYBERANGRIFFSALLEEN
Gebiet Eins: Hardware-Verwundbarkeiten
Allee 1: Physische Ausrüstung
Allee 2: Physische Umgebung
Allee 3: Physische Nebenprodukte
Gebiet Zwei: Softwarezugriffsverwundbarkeiten
Allee 4: Identitätsüberprüfung
Allee 5: Anwendungsvorzüge
Allee 6: Eingangsgültigkeitserklärung
Allee 7: Passende Verhaltensmuster
Gebiet Drei: Netzverwundbarkeiten
Allee 8: Dauerhafte Netzverbindungen
Allee 9: Periodisch auftretende Netzverbindungen
Allee 10: Netzwartung

Gebiet Vier: Automationsverwundbarkeiten
Allee 11: Entfernte Sensoren und Regelsysteme
Allee 12: Datensicherheitsvorgänge
Gebiet Fünf: Menschliche Bedienerverwundbarkeiten
Allee 13: Menschliche Wartung von Sicherheitsverfahren
Allee 14: Absichtliche Handlungen die Sicherheit drohend sind
Gebiet Sechs: Softwareversorgungsverwundbarkeiten
Allee 15: Innere Richtlinien für die Softwareentwicklung
Allee 16: Richtlinien die sich mit Außenverkäufern befassen

Innerhalb der sechzehn Alleen gibt es weitere Überschriften, die die Gegenmaßnahmen für die Schätzung der Angriffsalleen sammelt. Alle individuellen Verwundbarkeiten in der Kontrollliste werden in Bezug auf die Gegenmaßnahmen beschrieben, die genommen werden sollten, um die Verwundbarkeiten zu eliminieren oder zu minimieren. Ein Frageformat wurde genutzt, sodaß der Prüfer der den Artikel überprüft wissen wird das die richtigen Maßnahmen ergriffen worden sind, wenn die Antwort auf die Frage "ja" ist. Die Wörter in einigen der Fragen, die ungenau, wie "strikt", "gründlich", "ausreichend", und "genügend" klingen könnten, haben wirklich ziemlich genaue Bedeutungen in den Zusammenhängen, wo die angewendet werden. In den meisten Fällen, um diese Ausdrücke richtig zu interpretieren, ist es nur notwendig zu fragen, "was soll diese Gegenmaßnahme erreichen?" und dann kann man sehen ob die ausreichende Maßnahme genommen wurde um den Zweck zu erreichen.

Es wurde Acht gegeben, die zurzeit modernen Phrasen zu vermeiden und technischen Jargon zu einem Minimum zu halten. Statt dessen ist jede Anstrengung gemacht worden, um zu sagen was gemeint ist, als klar und geradeheraus als möglich, übereinstimmend mit der Kürze. Wenn jemand nach einem Cybersicherheitsproblem durch ein zurzeit modernes Modewort sucht, ist es fast immer hier, aber die Modewörter selbst werden nicht da sein.

Viele Fragen über "korporative Richtlinien" und "Bestätigungen" sind aus dieser Kontrollliste absichtlich weggelassen worden mit der Begründung, dass diese Punkte gewöhnlich als selbstverständlich betrachtet werden sollten. *Jede* in dieser Kontrollliste

enthaltenen Sicherheitsmaßnahmen sollten als Angelegenheiten der korporativen Politik ausgeführt werden. *Jede* in dieser Kontrollliste enthaltenen Sicherheitsmaßnahmen sollten einer Überprüfung unterworfen werden. Dieser Punkt soll sicherstellen, daß die Sicherheitsmaßnahmen in der Kontrollliste wirklich ausgeführt werden. Richtlinien und Überprüfungen sind nur zusätzliche Elemente um das zu erreichen. Wo die Kontrollliste ausdrücklich erwähnt, "korporative Politik" oder "Überprüfungen", das fragliche Problem bekommt dann eins wo spezielle Prozeduren errichtet werden müssen. Normalerweise werden die Grundsätze einer guten Verwaltung die notwendigen Richtlinien und Überprüfungen andeuten.

Die administrativen und organisatorischen Maßnahmen notwendig, um gute Cybersicherheitspraxen durchzuführen, sind auch größtenteils aus dieser Kontrollliste weggelassen worden. Das ist so da diese Maßnahmen die wirksame Entwicklung von Rollen, Verantwortungen, Antrieb, und Befehlsketten betrifft, diese sind alle Betriebsleitungspraktiken, nicht Cybersicherheit spezifische Praktiken. Einige Grundsätze und Richtlinien für die Verwaltung von Cybersicherheitsbestimmungen sind in anderen von der U.S. Cyber Konsequenzen Abteilung erzeugten Dokumenten ausgelegt worden. Aber es gibt wirklich viele verschiedene Verwaltungsmaßnahmen die verwendet werden können um dieselben Cybersicherheitsmaßnahmen durchzuführen.

Obwohl sich das Dokument überall auf "Gesellschaften" und auf "Geschäfte" bezieht, sollten diese Begriffe sehr allgemein interpretiert werden. Jede Organisation, die ein Budget und Informationssysteme hat und versucht, praktische Tätigkeiten auszuführen, kann als eine "Gesellschaft" zum Zwecke der Cybersicherheit behandelt werden. Das schließt Regierungsstellen und Agenturen, gemeinnützige Gesellschaften, und die meisten anderen nichtstaatlichen Organisationen auch ein. Die "Handlungen", die diese Organisationen ausführen, können irgendwelche Tätigkeiten sein, die Werte erschaffen oder liefern, unabhängig davon ob diese Werte jemals finanziell beurteilt oder beschrieben werden. Der Grund für den gewählten Ausdruck "Gesellschaften" ist das die größten Teile der Informationssystemen der Nationen im Besitz und unter Verwaltung der Gesellschaften sind.

Viele Gesellschaften werden finden, dass nicht alle Fragen in der Kontrollliste sich ihren Informationssystemen zutreffen. Einige Gesellschaften werden, zum Beispiel, die verschiedenen Fernsensoren und Regelsysteme, welche der Fokus für die meisten Fragen in der Allee 11 sind, nicht benutzen. Andere Gesellschaften werden finden, dass es für sie nicht praktisch ist, die physisch getrennten Datenzentren, die in vielen der Fragen erwähnt werden, aufrechtzuerhalten. Dennoch werden andere Gesellschaften finden, dass sie keine Systeme haben, die so äußerst kritisch sind, um die sehr aufwändigen in der Kontrollliste

beschriebenen Sicherheitsmaßnahmen zu gewähren. Bevor ein Artikel als "nichtanwendbar" erklärt wird, sollte eine Gesellschaft sicherstellen, dass der Artikel nicht zu einer übersehenen Verwundbarkeit hinweist. Eigenschaften eines Informationssystems, die in einer speziellen Industrie nicht auffällig sind, können noch eine grosse Sicherheitsverwundbarkeit für diese Industrie darstellen.

Die Gegenmaßnahmen gekennzeichnet mit einem Sternchen *sind zurzeit sehr schwierig oder sehr teuer wenn die mit den Produkten und Technologien die routinemäßig von kommerziellen Verkäufern vorhanden sind, implementiert werden. Das bedeutet, dass, vorläufig mindestens, sie spezielle Initiativen von der improvisierten Hardware zum Beauftragen der kundenspezifischen Programmierung verlangen. Sicherheitsverkäufer, Regierungsstellen, und Einrichtungen, die Sicherheit R&D finanziell unterstützen, sollten diese mit Sternchen gekennzeichneten Artikel besonders beachten. Die sind an allen Plätzen, wo neue Produkteigenschaften oder neue Dienstleistungen, um Informationssicherheit zu verbessern, dringend benötigt sind.

In Situationen, wo diese Kontrollliste der US-CCU als ein Standard für die Informationssicherheitseinhaltung verwendet wird, sollten die mit Sternchen gekennzeichneten Artikel als wahlweise behandelt werden. Im Laufe der kommenden Monate und Jahre, als neue Technologien, Produkte, und Dienstleistungen verfügbar sein werden und die Kontrollliste regelmäßig aktualisiert wird, viele der Sternchen werden zweifellos entfernt, und Artikel, die zurzeit wahlweise sind, werden allmählich ein Teil der Standardsicherheitspraxen bekommen. In der Zwischenzeit ist es nicht praktisch zu erwarten dass Gesellschaften Sicherheitsprobleme bewältigen, wo Standardlösungen nicht routinemäßig angeboten werden, diese Probleme können trotzdem sehr wichtig sein.

Einige der Artikel in der Kontrollliste, die nicht mit einem Sternchen gekennzeichnet sind, können sich schwierig oder teuer anhören, aber in den meisten Fällen ist das eine Illusion. Es ist wahr, dass es einige sehr teure Weisen gibt, um diese Verwundbarkeiten unter Kontrolle zu bringen und einige sehr teure Produkte werden angeboten um die Verwundbarkeiten zu behandeln. Aber für eigentlich alle Artikel ohne ein Sternchen gibt es auch relativ billige Weisen um diesen Sicherheitsbedarf zu befriedigen

Wenn Cybersicherheit in Bezug auf ein "Risikodreieck" beschrieben wird, wo die drei Ecken Drohungen, Folgen, und Verwundbarkeit sind, befasst sich diese Kontrollliste nur mit der Verwundbarkeit. Um diese Kontrollliste in einer preisgünstigen Weise anzuwenden, ist es notwendig, die anderen Ecken des Risikodreiecks in Betracht zu ziehen. Das bedeutet das die Drohungen genügend verstanden werden müssen, um eine Idee zu haben welche verschiedenen Angriffe, im Laufe einer gegebenen Zeitspanne erwarten werden können. Noch wichtiger ist es die Konsequenzen zu verstehen, um zu

wissen wie kritisch die verschiedenen Softwareanwendungen sind, wie empfindlich die verschiedenen Informationen sind, und welcher Sicherheitsverbrauch gerechtfertigt ist um die alle zu schützen. Obwohl diese Themen außerhalb der Reichweite der Cybersicherheitskontrollliste sind, werden die etwas umfänglich erklärt in Scott Borg's (bald erscheinenden) buchlangen Bericht: *Cyberangriffe: Ein Handbuch um die wirtschaftlichen und strategischen Gefahren zu verstehen*.

Diese Cybersicherheitskontrollliste der US-CCU beabsichtigt nicht alle vorherigen Verwundbarkeitskontrolllisten zu ersetzen oder andere Listen unnötig zu machen. Wahrhaftig, um diese Übersichtsliste durchzuführen, wird es allgemein notwendig sein, zusätzliche, spezialisierte Kontrolllisten zu verwenden, die mehr Detail auf die spezifischen Sicherheitsproblemen, auf die letzten technischen Entwicklungen, und auf den speziellen Voraussetzungen von individuellen Industrien zur Verfügung stellen. Es wird jedoch gehofft, dass diese Liste der US-CCU helfen wird die Aufmerksamkeit auf viele Verwundbarkeiten zu lenken, die sonst überblickt werden könnten.

Gebiet Eins: Hardware-Verwundbarkeiten

Allee 1: Physische Ausrüstung

Die Verfolgung Physischer Ausrüstung

- 1.01. Erhält die Gesellschaft einen genauen Warenbestand der elektronischen Ausrüstung in jedem Zimmer an jeder physischen Stelle aufrecht?
- 1.02. Gibt es ein schnelles und leichtes Verfahren, um diesen Warenbestand zu aktualisieren, wenn auch immer ein Angestellter mit der Verantwortung für ein Teil der Ausrüstung die Bewegung berechtigt?
- 1.03. Ist jedes Stück der elektronischen Ausrüstung etikettiert mit einem Strichcode oder anderem Bezeichner für die einfache Verfolgung?
- 1.04. Wenn Informationsausrüstung genügend empfindlich ist, wird es mit den Rundfunkfrequenz-Identifizierung (RFID) Chips markiert, so dass ihre Bewegungen fast in der Echtzeit verfolgt werden können? *
- 1.05. Gibt es eine ausführliche Richtlinie, die angibt, welche Ausrüstungen von den Gesellschaftslokalen weggenommen werden können, und welche Genehmigungen erforderlich sind, um die zu entfernen?
- 1.06. Wenn elektronische Ausrüstung von den Gesellschaftslokalen weggenommen werden muß, gibt es ein wirkungsvolles Verfahren, um die Bewegung dieser Ausrüstung zu verfolgen?

- 1.07. Werden unangemeldete Stichproben regelmäßig ausgeführt, um nachzuprüfen, daß die elektronische Ausrüstung in den Ausrüstungswarenbestand bezeichneten Positionen anwesend ist?

Bewachung Physischer Ausrüstung

- 1.08. Sind besonders wichtige Stücke der elektronischen Ausrüstung konsolidiert in Datenzentren für die einfachere Schützung?
- 1.09. Sind physische Sicherheitssperren errichtet worden um elektronische Ausrüstung vor dem Diebstahl oder böswilligem Schaden zu schützen?
- 1.10. Wenn äussere Festplatten und andere äussere Datenspeicherungsgeräte empfindliche Information enthalten und es einfach sein würde die fortzutragen, werden die als eine extra Sicherheitsvorsichtsmaßnahme veränkert? *
- 1.11. Sind Verteilerschränke zu jeder Zeit sicher geschlossen?
- 1.12. Sind das Datenzentrum und die Verteilerschränke mit einem Eindringungsalarm ausgerüstet?
- 1.13. Werden die Eindringungsalarme für das Datenzentrum und die Verteilerschränke von außen überwacht?
- 1.14. Ist physischer Zugang zu den Konsolenverbindungen von Sicherheitsgeräten, wie diese die zur Verwaltung von Brandmauern und Eindringungsentdeckungssystemen benutzt werden, eingeschränkt auf autorisierte Benutzer?
- 1.15. Sind da irgendwelche abgehängte Decken oder erhobene Fußböden im Datenzentrum und anderen Gebieten, die kritische Informationsausrüstung unterbringt, gegen den Zugang von angrenzenden Räumen und Lüftungssystemen gesichert?

Schützung Elektronischer Zugriffspoints

- 1.16. Werden unbenutzte Netzzugriffspoints durch Netzschalter oder physische Sicherheitssperren ausgeschaltet, um unberechtigten Zugang zu verhindern?
- 1.17. Wo die Netzports nicht wirklich ausgeschaltet werden, sind dort Verfahren, um den unberechtigten Zugang zu diesen Ports zu bewachen?
- 1.18. Gibt es physische Sicherheitssperren, wie geschlossene Deckel oder Stecker, um alle Medienzugriffspunkte des Systems (z.B, USB Ports, CD-Antriebe, usw.) zu schützen? *
- 1.19. Wo die Medienports nicht wirklich ausgeschaltet werden, sind dort Verfahren, um den unberechtigten Zugang zu diesen Ports zu überwachen? *
- 1.20. Ist der physische Zugang zu allen unbenutzten Ports auf Netzschaltern ausgeschaltet worden, besonders der Switched Port Analyzer (SPAN) Port?

- 1.21. Ist der physische Zugang zu allen Konsolen und Nebenports auf Routern geschützt?

Schätzung der Kommunikationslinien

- 1.22. Sind physische Sicherheitssperren errichtet, um die Netzkabel zu schützen, die zu und vom System laufen, so dass die nicht leicht getrennt oder beschädigt werden können?
- 1.23. Sind die kritischen Kommunikationskabel und Kabelbäume innerhalb der Gesellschaftseinrichtungen so gelegt das es schwierig ist physischen Zugang zu haben um Übermittlungen abzufangen?
- 1.24. Gibt es physischen Schutz am Demarc-Punkt, wo Telefon und Datenkabel ins Gebäude eingehen?
- 1.25. Untersucht die Gesellschaft die physischen Sicherheitsverfahren von Internetdienstversorgern und anderen Kommunikationsgesellschaften bevor wählen von welcher Gesellschaft, Dienstleistungen zu kaufen?

Regeln wie Ausrüstung physisch zugegriffen wird

- 1.26. Wird das Datenzentrum zu jeder Zeit sicher abgeschlossen, mit Türen an Zugangspunkten die geschlossen bleiben?
- 1.27. Hat das Datenzentrum "begrenztes Gebiet" Schilder an den Zugangstüren?
- 1.28. Ist Zugang zum Datenzentrum kontrolliert mit Technologien wie abtastbare Kennzeichen, Smart Cards, Näherungskarten, Biometrie, oder Schlösser, die persönliche Kombinationen verlangen?
- 1.29. Sind die Logs für die Zugriffskontrollmechanismen (z.B, Schlüsselkarten und Videokontrolllogs) regelmässig nachgeprüft?
- 1.30. Schließt diese Überprüfung eine Analyse von erfolglosen physischen Zugriffsversuchen ein?
- 1.31. Wird Videoüberwachung verwendet, um Zugangsportale für Datenzentren und anderen Bereichen die Informationsverarbeitungsanlagen unterbringen, zu beobachten?
- 1.32. Falls es Videoüberwachung der Datenzentren gibt, wird es von außerhalb des Gebäudes kontrolliert?
- 1.33. Falls es Videoüberwachung der Datenzentren gibt, wird das Video in einem dauerhaften Medium aufgenommen sodaß damit nicht herumgepuscht werden kann?
- 1.34. Falls es Videoüberwachung der Datenzentren gibt, werden die Videoaufnahmen lange genug behalten, sodaß die noch verfügbar sein würden, um eine

Sicherheitsübertretung die für mehrere Monate nicht entdeckt wurde, zu untersuchen?

- 1.35. Wenn Sicherheitskameras, besonders drahtlose, für die Überwachung verwendet werden, werden die vor der Klemmung, der unberechtigten Betrachtung, und dem spoofing von Bildern geschützt? *
- 1.36. Ist Zugang zu den Verwaltungskonsolen von Sicherheitselementen, wie Brandmauern und IDS, physisch eingeschränkt auf autorisierte Benutzer?
- 1.37. Wird physischer Zugang zu allen drahtlosen und infraroten Netzzugangsgeräten überwacht und kontrolliert?
- 1.38. Sind Faxgeräte die empfindliche Informationen empfangen und drucken gegen unberechtigten Zugang geschützt?

Überwachen welches Personal physischen Zugang hat

- 1.39. Gibt es Regeln über wer in das Gebäude wo das Informationssystem operiert hinein geht und heraus kommt?
- 1.40. Gibt es klare und strikt erzwungene Beschränkungen, für welche Angestellte Zugang zum Datenzentrum haben?
- 1.41. Gibt es klare Regeln und strikte Kontrollen für den Zugang zu den Verteilerschränken?
- 1.42. Sind da strikte Kontrollen die physische Zugangsprivilegien modifizieren, wenn sich die Rolle eines Angestellten ändert?
- 1.43. Sind physische Zugangsprivilegien und Elemente sowie Kennzeichen sofort deaktiviert, wenn ein Angestellter gekündigt wird, weggeht, oder in den Ruhestand geht?
- 1.44. Gibt es strikte Kontrollen für den Zugang der Lieferanten zum Datenzentrum, sodaß nur richtig autorisierte Lieferanten hereingelassen werden?
- 1.45. Hat das Datenzentrum ein Anmeldeverfahren das verwendet wird, um Nichtangestellte in den begrenzten Raum einzubuchen?
- 1.46. Werden physische Zugangsprivilegien und Geräte für Lieferanten oft nachgeprüft und schnell deaktiviert, wenn es Änderungen im Status des Lieferantenpersonal gibt?
- 1.47. Gibt es strikte Richtlinien, die das Verfahren für den Zugang zum Datenzentrum nach Betriebszeiten bei Personal wie zum Beispiel Raumpfleger, umfassen?
- 1.48. Gibt es korporative Sicherheitsrichtlinien für den Notzugang zum Datenzentrum?

Allee 2: Physische Umgebung

Umgebungskontrollen

- 2.01 Gibt es Umgebungskontrollen, wie die Heizung und Kühlsysteme, die eine stetige Betriebstemperatur für die elektronische Ausrüstung aufrechterhalten können?
- 2.02 Ist die elektronische Ausrüstung vor der Feuchtigkeit oder übermäßiger Luftfeuchtigkeit geschützt?
- 2.03 Falls die Umgebungskontrollen von entfernt verwaltet werden können, werden diese Kontrollen vor dem unberechtigten Zugang entsprechend geschützt?
- 2.04 Gibt es Umgebungskontrollen die das System vor Elementen wie Rauch, Staub, und chemische Ausströmungen schützen?
- 2.05 Gibt es Umgebungssensoren, besonders für Temperatur, Rauch, und Feuchtigkeit im Datenzentrum und in den Verteilerschränken?
- 2.06 Sind die Gebiete, die elektronische Ausrüstung storen ausgestattet mit einem für die elektronische Ausrüstung passenden Feuerunterdrückungssystem?
- 2.07 Gibt es Feuerunterdrückungssysteme die Feuersbrünste in den benachbarten Gebieten kontrollieren?

Energieversorgung

- 2.08. Werden Notstromabsperungsschalter auffallend gekennzeichnet, mit Video kontrolliert, und mit Sicherheitsplatten bedeckt, um es zu verhindern das die elektrische Energie unpassend unterbrochen wird?
- 2.09. Sind physische Sicherheitssperren gegründet worden, um die in Verbindung stehenden Stromkabel in der Nähe vom Datenzentrum zu schützen, sodaß sie nicht leicht getrennt oder beschädigt werden können?
- 2.10. Sind Maßnahmen genommen worden, um die in Verbindung stehenden Stromkabel weiter weg vom Datenzentrum nicht durch, sogleich identifizierbare, unsichere Plätze zu führen?
- 2.11. Sind elektrische Versorgungsbestandteile, wie Stromplatten und Stromkreisunterbrecherkästen, von dem unberechtigten Zugang geschützt?
- 2.12. Wenn ununterbrochene Energieversorgung (UPS'S) verwertet wird wird diese von dem autorisierten entfernten Zugang geschützt?
- 2.13. Wenn die Systeme kritisch genug sind, werden die durch zwei verschiedene Verbindungswege zum Strom verbunden?
- 2.14. Werden Aushilfsgeneratoren mit Sicherheitsgeräten, wie Schlösser, Warnungen, und Stacheldrahtzaeunen geschützt?

- 2.15. Gibt es eine entsprechende Aushilfsenergieversorgung besonders für Betriebskritischen Systemen?
- 2.16. Hat die Aushilfsenergieversorgung genügend Brennstoff für eine ziemlich lange Unterbrechung in der Kraftstoffversorgungskette?
- 2.17. Wird die Aushilfsenergieversorgung unter einer Volllast regelmäßig geprüft und ist die lange genug an um nachzuprüfen, dass alles in Arbeitsordnung ist?
- 2.18. Ist die Aushilfsenergieversorgung in einer Position die nicht gegen Überschwemmung anfaellig ist?
- 2.19. Gibt es Schutz gegen extreme Stromstösse die durch einen Blitz oder vielleicht durch künstliche Mittel erzeugt werden koennten?

Allee 3: Physische Nebenprodukte

- 3.01. Sind Dokumente die empfindliche Information enthalten geschützt damit die nicht gedruckt werden wenn es kein betriebliches Bedürfnis dafuer gibt? *
- 3.02. Sind da ausreichend strikte Verfahren die den Zugang zu Papierdruckausgaben die empfindliche Informationen enthalten beschraenken?
- 3.03. Sind da korporative Sicherheitsrichtlinien die definieren welche Aufbewahrungsbehälter fuer Papierdruckausgaben mit empfindlichen Informationen verwendet werden koennen?
- 3.04. Gibt es ausreichend strikte Verfahren für die sichere Vernichtung von Papierdruckausgaben?
- 3.05. Hat man beachtet das Papierwiedergebrauch- und Wiederverwertungsprogramme nicht andere Sicherheitshandlungen der Papierdruckausgaben schwaechen?
- 3.06. Gibt es ausreichend strikte Richtlinien und Verfahren die den Gebrauch von entfernbaren magnetischen Medien, wie Universeller serieller BUS (USB) Geräte, regeln?
- 3.07. Gibt es ausreichend strikte Verfahren um unberechtigten Zugang zu Backup Medien zu begrenzen?
- 3.08. Gibt es ausreichend strikte Verfahren, um CD-ROM Disketten und entfernbare magnetische Medien die empfindliche Informationen enthalten, richtig zu inventarisieren?
- 3.09. Gibt es ein festgesetztes Verfahren, um die Entfernung von Artikeln vom Warenbestand der Speicherungsmedien zu dokumentieren, so dass die verantwortlichen Angestellten zuerst nachprüfen, dass die Medien für die Beseitigung entfernt wurden, zweitens das die richtig vernichtet oder sterilisiert wurden, und drittens das die materiellen Rueckstaende physisch erloest wurden.?

- 3.10. Gibt es ausreichend strikte Verfahren, um entfernbare Datenspeichergeräte die zu einer anderen Stelle ausserhalb des Gebaeudes bewegt werden muessen, richtig zu verladen?
- 3.11. Gibt es regelmäßige Verfahren um sicherzustellen, dass Speichermedien, wie Festplatten, Bänder, Flash Drives, und Zip Disketten, gründlich überschrieben werden, bevor sie dem verschiedenen Geschäftsgebrauch wiederzugeteilt werden?
- 3.12. Gibt es ausreichend strikte Verfahren für die sichere Vernichtung oder Sterilizierung von Speichermedien, wie Festplatten, Bänder, Flash Drives, und Zip Disketten, wenn die aus dem Geschäftsdienst genommen werden?
- 3.13. Gibt es ausreichend strikte Verfahren, um Speichermedien zu sterilisieren, wenn die zurückgegeben werden für den Garantienersatz, um öffentlich verkauft zu werden, oder wenn die fuer den karitativen Gebrauch gestiftet werden?
- 3.14. Werden verwendete CD-ROM Disketten mit empfindlichen Informationen entsprechend vernichtet (nicht nur gebrochen) bevor der Beseitigung?

Gebiet Zwei: Softwarezugriffsverwundbarkeiten

Allee 4: Identitätsbeglaubigung

Beglaubigungsrichtlinien

- 4.01. Werden Informationssysteme mit grundlegenden Beglaubigungsmechanismen, wie Benutzername und Kennwort geschützt?
- 4.02. Ist der Zugang jedes Benutzers zu Anwendungen auf dem System eingeschaenkt zu diesen Anwendungen?
- 4.03. Wenn eine Anwendung Zugang zu empfindlichen Informationen erlaubt, verlangt es eine zusätzliche Benutzerbeglaubigung?
- 4.04. Wenn eine Anwendung kritisch genug ist oder die Informationen empfindlich genug sind, verwendet das System erweiterte Beglaubigungsmechanismen, wie Biometrie, zwei-Faktor Wertmarken, oder herausgeforderte Tauschungen?
- 4.05. Werden Terminals und Softwaresysteme festgesetzt, um den Benutzer auszusperrern und eine neue Anmeldung zu verlangen, wenn es da ein Zeitraum der Untätigkeit gibt, oder wenn ein anderes Gerät anzeigt, dass der Angestellte das Terminal verlassen hat?
- 4.06. Wenn ein kritisches System von einer Entfernung zugegriffen werden kann über eins oder mehrere dieser Beglaubigungsmechanismen, ist die Verbindung selbst geeignet oder encrypted?

- 4.07. Wenn erweiterte Beglaubigung als ein Zugriffsmechanismus verwendet wird, wird diese Technologie auf eine konsequente und wirksame Weise überall im Unternehmen angewendet?
- 4.08. Gibt es ein Verfahren, um die Rechte für zwei-Faktor Token und Smart Cards schnell zu widerrufen, wenn die kompromittiert werden?
- 4.09. Gibt es einen Warnungsmechanismus der ein Benachrichtigungssignal sendet, wenn ein Versuch gemacht wird eine zwei-Faktor Token oder Smart Card zu verwenden, nachdem die widerrufen worden ist?*
- 4.10. Wenn Biometrie verwendet wird, ist eine persönliche Geheimnummer auch verlangt, um Identität nachzuprüfen?
- 4.11. Wenn Biometrie verwendet wird, werden live-scans oder andere Messungen gemacht, um zu prüfen, dass das Lesen von einer echten Person genommen wird?*
- 4.12. Falls es notwendig ist, hat die Gesellschaft einen Weg, Daten und Anwendungen normalerweise geschützt durch persönliche zwei Faktor-Token wie biometric Beglaubigung zuzugreifen? *

Die Überwachung von Zugriffen und Zugriffsversuchen

- 4.13. Verlangen korporative Richtlinien, daß alle Zugriffsversuche gelogged werden, unabhängig davon, ob die erfolgreich oder erfolglos sind, besonders für Anwendungen die kritische Funktionen ausführen oder empfindliche Informationen speichern?
- 4.14. Werden alle Änderungen, die ein Systemadministrator an Kennwörtern macht geloggt und nachgeprüft?
- 4.15. Sind alle Steigerungen in Zugriffsrechten geloggt und nachgeprüft?
- 4.16. Gibt es einen Warnungsmechanismus der warnen würde wenn das allgemeine Hauptlevel oder Administratorlevel (z.B, Bereichsadministrator) Konto benutzt wird?
- 4.17. Werden alle Zugriffslogs zu einer unüberschreibbaren Diskette oder anderem dauerhaftem Medium geschrieben, wo sogar der Systemadministrator an denen nicht herumfuschen kann? *
- 4.18. Werden erfolgreiche Beglaubigungen nachgeprüft, um sicherzustellen, dass der Zugang richtig und geeignet war?
- 4.19. Wird sich Mühe gemacht erfolgreiche Zugriffsversuche zu identifizieren und zu untersuchen wenn die in ungewöhnlichen Stunden des Tages oder der Nacht ausgeführt werden?
- 4.20. Werden vielfache erfolglose Zugriffsversuche zeitgemäß nachgeprüft?

- 4.21. Gibt es automatische Warnungen und Verteidigungsmaßnahmen, die entworfen wurden um Angriffe brutaler Gewalt gegen die Anmelde-mechanismen zu entgegenen und anzusteuern durch vielfache Anmelde-versuche, selbst wenn die über einen Zeitraum oder über Benutzeridentifikationen verteilt werden?

Management von Kennwörtern und Biometrie

- 4.22. Verlangen korporative Richtlinien sichere Verfahren, um Kennwörter auszugeben?
- 4.23. Definieren korporative Richtlinien minimale Kennwort Länge, Beobachtung der Rolle des Benutzers, und welche Länge-Kennwörter die fraglichen Systeme unterstützen werden?
- 4.24. Werden Anwendungen entwickelt innerhalb der Gesellschaft, und mit Kennwörtern geschützt die eine minimale und maximale Zahl von Buchstaben haben?
- 4.25. Beauftragen korporative Richtlinien Kennwort-Kompliziertheitsvoraussetzungen, eine Mischung von Buchstaben-Typen oder Buchstaben die von einem grossen Buchstaben Satz gewählt wurden?
- 4.26. Ist man vorsichtig, nicht die Kennwörter im klaren Text durch die E-Mail oder Instant Messaging zu schicken?
- 4.27. Sind Angestellte verpflichtet, ihre Kennwörter täglich zu ändern als angeordnet durch korporative Regeln?
- 4.28. Werden Angestellte gehindert, vorherige Kennwörter zu verwenden, wenn eine geplante Kennwort-Änderung benötigt ist?
- 4.29. Beauftragen korporative Richtlinien entsprechende Kennwortbedürfnisse, für die Netzwerkausrüstung, wie Router und Schalter?
- 4.30. Sind Maßnahmen ergriffen worden, um jemanden davon abzuhalten, Kennwörter durch den Diebstahl einer verschlüsselten oder unverschlüsselten Datei zu erhalten, in welcher die gespeichert werden?
- 4.31. Gibt es einen Warnungsmechanismus der vor dem Diebstahl einer Datei, in welche Kennwörter gespeichert werden, warnen würde? *
- 4.32. Gibt es ein Verfahren für die schnelle und sichere Änderung von Kennwörtern, falls es irgendwelchen Grund gibt zu glauben, daß die kompromittiert worden sind?
- 4.33. Beauftragen korporative Sicherheitsrichtlinien die unmittelbare Deaktivierung von Kennwörtern, wenn ein Angestellter gekündigt wird, weggeht, oder in den Ruhestand geht?

- 4.34. Sind Server und Arbeitsstationsanwendungen regelmäßig revidiert um Kontos zu identifizieren die unbenutzt sind oder die ehemaligen Angestellten zugeteilt wurden und um sicherzustellen, daß diese Kontos entfernt worden sind oder neue Kennwörter zugeteilt worden sind?
- 4.35. Gibt es einen strikten Registrierungsprozess für biometric Identifikatoren, so dass es hochgradiges Vertrauen gibt daß die aufgenommenen Daten von der richtigen Person sind?
- 4.36. Sobald eine biometric Information eines Benutzers aufgenommen wird, wird es in einen sicheren Platz gespeichert wo Diebstahl und herumpfuschen verhindert werden kann?
- 4.37. Haben die Gesellschaft und ihre Lieferanten einen Plan, um kompromittierte biometric Information mit der alternativen Information auszutauschen? *
- 4.38. Definieren korporative Richtlinien die Verfahren, um sich mit der Vernichtung der nicht mehr benötigten biometric Informationen, zu befassen?

Management von Verschlüsselungsschlüsseln und Digitalzertifikaten

- 4.39. Werden Verschlüsselungsschlüssel auf eine sichere Weise entworfen, entsprechend genehmigter Industriemethoden?
- 4.40. Werden Dekodierungsverfahren getrennt von Anmeldeverfahren aktiviert und erfordert verschiedene Kennwörter zu verwenden?
- 4.41. Ist die Erzeugung von Verschlüsselungsschlüsseln in einer einbruchssicheren Datei geloggt die die Mitarbeiteridentität und die Zeit einträgt?
- 4.42. Sind Verschlüsselungsschlüssel und Digitalzertifikate auf eine sichere Weise verteilt um Diebstahl zu verhindern?
- 4.43. Werden Verschlüsselungsschlüssel auf eine sichere Weise gespeichert, entsprechend genehmigter Industriemethoden?
- 4.44. Werden Verschlüsselungsschlüssel auf eine sichere Weise zerstört, entsprechend genehmigter Industriemethoden?
- 4.45. Gibt es ein schnelles und wirksames Verfahren, um sich mit kompromittierten Verschlüsselungsschlüsseln zu befassen?
- 4.46. Gibt es regelmäßige und zuverlässige Verfahren für das Archivieren von privaten Verschlüsselungsschlüsseln und vereinigten Pass-Ausdrücken für individuelle Benutzer?
- 4.47. Wenn private Verschlüsselungsschlüssel aufrechterhalten werden, werden die in einem Kennwort geschützten und verschlüsseltes Gebiet archiviert, um Diebstahl und herumbasteln zu verhindern?

- 4.48. Sind Archive der privaten Verschlüsselung und vereinigten Pass-Ausdruck-Schlüsseln aufrechterhalten, nachdem sie nicht mehr im aktiven Gebrauch sind, so vorher verschlüsselte Dateien können nötigenfalls wiedergefunden werden?
- 4.49. Definieren korporative Richtlinien die Verfahren, um Digitalzertifikatbeglaubigungsmechanismen einzusetzen?
- 4.50. Sind Kopien der privaten Schlüssel von Digitalzertifikaten in einem Kennwort geschützten und verschlüsseltem Gebiet gespeichert das die Wiederherstellung erlaubt und Diebstahl verhindert?
- 4.51. Haben Systeme mit installierten Zertifikaten entsprechende Sicherheitsmaßnahmen die den Diebstahl der privaten Schlüssel dieser Zertifikate verhindert?
- 4.52. Gibt es ein Verfahren das erlaubt kompromittierte private Schlüssel von Digitalzertifikaten, schnell widerzurufen?
- 4.53. Haben Verschlüsselungsschlüssel und Digitalzertifikate Ablaufzeiträume?

Management der Dokumenten Authentizität

- 4.54. Sind Dokumente die die Arbeit oder Stellungen der Gesellschaft zeigen, umgewandelt in Formate die nicht leicht modifiziert werden können, bevor die elektronisch außerhalb der Gesellschaft in Umlauf gesetzt werden?
- 4.55. Werden Dokumente digital unterzeichnet, wenn die in Formate umgewandelt werden, die nicht leicht modifiziert werden können?
- 4.56. Werden die Digitalunterschriften auf wichtigen Dokumenten regelmäßig überprüft um nachzuprüfen daß die Dokumente wirklich von der selben Person erschaffen wurden?
- 4.57. Werden wichtige E-Mails gesendet, mit der Benutzung einer Anwendung die den Inhalt zerlegt und eine Digitalunterschrift hinzufügt, sodaß der Inhalt der E-Mails und die Identität des Absenders nicht leicht gefälscht werden können?
- 4.58. Werden Einnahmen für wichtige E-Mails gesammelt und gespeichert, um eine Eintragung zur Verfügung zu stellen, die nachprüft daß der Empfänger erreicht wurde?

Allee 5: Anwendungsprivilegien

Anpassung von Privilegien

- 5.01. Werden die Standardsicherheitseinstellungen auf den Software- und Hardwaregeräten geändert, bevor diese Geräte in Betrieb gesetzt werden?
- 5.02. Hat die Gesellschaft ausdrücklich Kritikalität Klassifikationen zu den wichtigeren oder mehr verwendeten Softwareanwendungen zugeteilt?

- 5.03. Ist Zugang zu kritischen Anwendungen eingeschränkt auf diejenigen Benutzer innerhalb der Gesellschaft die wirklich diese Anwendungen benutzen müssen?
- 5.04. Hat die Gesellschaft Empfindlichkeitsklassifikationen den Informationsdateien zugeteilt?
- 5.05. Ist Zugang zu empfindlichen Daten eingeschränkt auf diejenigen Benutzer innerhalb der Gesellschaft die wirklich diese Daten benutzen müssen?
- 5.06. Ist die Fähigkeit Daten in Dokumenten oder Dateien zu verändern oder einzugeben auf diejenigen Angestellten eingeschränkt die im Laufe ihrer normalen Arbeit einen gültigen Bedarf haben?
- 5.07. Ist die Fähigkeit Ausgänge mit empfindlichen Informationen herzustellen, wie gedruckte Fassungen und E-Mail-Attachments, eingeschränkt zu was der Job und die Verantwortungen des Benutzers benötigen würde?
- 5.08. Werden Hauptlevel- und Administratorlevelprivilegien auf diejenigen eingeschränkt die wirklich den Bedarf für diese Privilegien haben?
- 5.09. Werden Hauptlevel- und Administratorlevelprivilegien kontrolliert und revidiert?
- 5.10. Gibt es einen dokumentierten Genehmigungsprozess, um Leuten Zugang zu virtuellen privaten Netzwerken zu geben?
- 5.11. Gibt es einen dokumentierten Genehmigungsprozess, um Leuten entfernten Zugang zu Modems zu geben?
- 5.12. Gibt es ein Verfahren, um zu dokumentieren und zu verfolgen, welche Privilegien für jeden individuellen Angestellten aktiv sind?
- 5.13. Sind die Softwareanwendungsprivilegien für individuelle Angestellte nachgeprüft und revidiert, wenn immer es eine wesentliche Änderung in ihren Arbeitsauftraegen gibt?
- 5.14. Gibt es ein Verfahren, fuer die Entfernung und die Nachpruefung der Entfernung von Privilegien wenn die nicht mehr benoetigt werden?

Allgemeine Kontrolle von Privilegien

- 5.15. Werden Angestellte gehindert, empfindliche Information zu lokalen Speichergeräten, wie Floppy Discs, CD-ROM, oder USB-Laufwerke zu speichern abgesehen von Fällen wo Geschäftsbedürfnisse das verlangen? *
- 5.16. Werden Anwendungen kontrolliert, um zu bestimmen, ob empfindliche Information gedruckt, gespeichert, oder heruntergeladen werden, ohne unbestrittene Ursache? *
- 5.17. Werden oertlich gespeicherte kritische Datendateien normalerweise in einer verschluesselten Form behalten wenn nicht im Gebrauch? *

- 5.18. Kann ein gültiger Benutzer empfindliche Daten unsachgemaess von einem System zum anderen System laden oder herunterladen?
- 5.19. Sind alle Hochladungen von empfindlichen Datendateien kontrolliert und geloggt?
- 5.20. Sind alle Hochladungen von verschlüsselten Datendateien kontrolliert und geloggt?
- 5.21. Sind da Bestimmungen die gültige Benutzer davon abhalten, ausführbare Dateien zu ihrem System herunterzuladen, ohne das diese Dateien zuerst für Schaden verursachende Software gescannt werden?
- 5.22. Falls Angestellte empfindliche Information zu einem örtlichen Laufwerk speichern können, wird diese Handlung kontrolliert und geloggt? *
- 5.23. Kann ein gültiger Benutzer eingeschränkte Mittel auf andere Systeme ohne zusätzliche Kennwörter und/oder Gültigkeitserklärung durch die IP-Adresse zugreifen?
- 5.24. Wenn eine Dienstanwendung geheim gehalten werden muß, für Konkurrenzwecken, wird es web-zugänglich nur für das vertraute Personal gemacht, aber nicht für die allgemeine Öffentlichkeit?

Allee 6: Eingabebestätigung

- 6.01. Werden die Buchstaben die in Kennwort-Feldern eingegeben werden getarnt, so dass die von Zuschauern nicht gelesen werden können?
- 6.02. Gibt es ein Programm, das Kennwörter überprüft, wenn die geschaffen werden, um sicherzustellen, daß die den Anforderungen für Kennwörter entsprechen?
- 6.03. Sind alle Eingabefelder in einer Anwendung eingeschränkt auf die passenden Buchstaben und Ausdrücken? (Z.B ein Sozialversicherungsnummern Feld sollte nichts anderes als Ziffern und Querstrichen erlauben.)
- 6.04. Sind alle Eingabefelder in einer Anwendung auf eine passende minimale und maximale Länge eingeschränkt? (Z.B ein Sozialversicherungsnummern Feld sollte nur neun Ziffern erlauben.)
- 6.05. Sind die Begrenzungen für was in die Eingabefelder geschrieben werden kann, genügend einschränkend, sodaß diese Felder ausführbare Instruktionen nicht akzeptieren werden?
- 6.06. Gibt es Begrenzungen für die Datenfelder der Datei die den Beschränkungen in den Feldern auf der Benutzerschnittstelle entsprechen, sodaß ungeeignete Daten und ausführbare Instruktionen nicht direkt in die Datei eingefügt werden?
- 6.07. Werden Datenfelder die selten geändert werden müssen "read only" gemacht, sobald der Dateneintrag als richtig nachgeprüft wurde?

- 6.08. Nachdem ein Datenfeld "read only" gemacht worden ist, ist da ein geeignetes Verfahren, um dieses Feld unter speziellen Verhältnissen zu korrigieren und um diese Korrektur nachzuprüfen?
- 6.09. Wurden die Fehlermeldungen richtig entworfen, sodaß die nicht Informationen über das innere Design und Konfiguration der Software enthüllen?
- 6.10. Sind die Fehler beseitigenden Eigenschaften unbrauchbar gemacht worden, sodaß die nicht einen Weg anbieten um Informationen über das innere Design und Konfiguration der Software zur Verfügung zustellen?
- 6.11. Sind die Dienstports für kritische Anwendungen konfiguriert, um Daten herauszufiltern, die außerhalb der richtigen Betriebsparameter für diese Anwendungen sind? *
- 6.12. Ist eine Stressprüfung gegen die Dienstports geführt worden die bei kritischen Anwendungen benutzt werden, um sicherzustellen, daß die nicht anfällig sind Überschwemmungen am Dienstportlevel zu puffern?
- 6.13. Gibt es standard Parameters für Eingaben die kritische Prozesse regeln, sodaß versuchte Eingaben außerhalb dieser Parameter entweder blockiert werden oder Bestätigung von einer anderen Quelle gebraucht wird? *

Allee 7: Geeignete Verhaltensmuster

- 7.01. Gibt es einen Warnungsmechanismen der warnt, wenn die Daten scheinbar eingegeben werden von Angestellten in Massen oder mit Verteilungen die mit den normalen Arbeitsmustern dieser Angestellten nicht übereinstimmt? *
- 7.02. Gibt es einen Warnungsmechanismen der warnt, wenn Dateien in ungewöhnlichen Mengen oder in Sequenzen zugegriffen werden, die mit dem normalen Arbeitsmustern nicht übereinstimmen? *
- 7.03. Gibt es einen Warnungsmechanismen der warnt, wenn Internetgeschäftstransaktionen ungewöhnliche Kombinationen von Kundenidentität, Rechnungsadressen und Lieferadressen einschliessen? *
- 7.04. Gibt es regelmäßige Verfahren, für Prüfungsanpassungen und Änderungen in Regelsystemen um sicherzustellen, daß die Änderungen die sich einander entsprechen, wirklich einander entsprechen? *
- 7.05. Wird sich Mühe gegeben, um erfolgreiche Zugriffsversuche zu identifizieren und zu untersuchen die in ungewöhnlichen Stunden des Tages oder der Nacht ausgeführt werden, wenn Computer nicht bevollmächtigte Prozesse unbemerkt ausführen können? *

- 7.06. Gibt es irgendwelche Bestimmung, um Situationen zu entdecken, in welche gefälschte Daten oder Instruktionen ohne feststellbare Intrusion eingefügt werden? *
- 7.07. Ist die Datei gestaltet sodaß empfindliche Informationen nicht überschrieben werden können ohne aufeinanderfolgende, zeitgestempelte Änderungen, die sicher archiviert werden? *
- 7.08. Gibt es einen Mechanismen, um alle Änderungen zu kritischen Dateien zu kontrollieren und zu loggen?
- 7.09. Wird der Log für Änderungen zu kritischen Dateien regelmäßig analysiert für ungewöhnliche Zugriffsmuster, einschließlich ungewöhnliche Zugriffszeiten und Frequenzen? *
- 7.10. Wenn die Protokollierung der Datenänderung durchgeführt worden ist, wird der Log für ungewöhnliche Modifizierungsmuster in den Dateien regelmäßig analysiert? *
- 7.11. Werden System und Sicherheitslogs in einem Weg aufrechterhalten der die davon abhält, modifiziert oder gelöscht zu werden, nachdem die gespeichert worden sind
- 7.12. Enthält das System Honey Token die aus unechten Dokumenten oder unechten Aufstellungen bestehen mit Mechanismen, um zu loggen, ob und wenn auf die zugegriffen wird? *
- 7.13. Gibt es einen automatischen Prozess, um Systeme für Zeichen das falsche Informationen eingefügt wurden, zu kontrollieren?*
- 7.14. Gibt es einen automatischen Mechanismen der Systeme unter Quarantäne stellt wenn die vielleicht mit falschen Informationen kontaminiert worden sind, ohne die zu schließen? *

Gebiet Drei: Netzverwundbarkeiten

Allee 8: Dauerhafte Netzverbindungen

Netzverbindungsintegrität

- 8.01. Ist das Netzwerk selbst durch Beglaubigungsverfahren gesichert, zusätzlich zum Sichern von Systemen im Netz?
- 8.02. Sind Maßnahmen ergriffen worden, um unberechtigte Systeme davon abzuhalten, mit dem Netzwerk leicht verbunden zu werden?
- 8.03. Wird der Netzverkehr regelmäßig kontrolliert, um normale Gebrauchsmuster zu gründen?
- 8.04. Wird der Netzverkehr für versteckte Nachrichtenkanäle regelmäßig kontrolliert?

- 8.05. Sind die Netzwerkanschlussbestandteile konfiguriert worden, um kritischere Kategorien des Verkehrs, wie Prozesskontrollinstruktionen, Vorrang vor weniger kritischen Kategorien des Verkehrs wie E-Mails zu geben?
- 8.06. Haben kritische Systeme überflüssige Kommunikationsverbindungen?
- 8.07. Haben Netze die very kritisch sind, Überflüssigkeit in der umschaltenden Struktur?
- 8.08. Wenn empfindliche Informationen über das Netz, ins Netz, oder aus dem Netz übersandt werden, werden die Übertragungen vom Abhören oder von Modifizierung während dem Transit durch die Verschlüsselung geschützt?
- 8.09. Definieren korporative Richtlinien, welche Datenkommunikationen verschlüsselt sein sollen, und welche Verschlüsselungstechnologien verwendet werden sollen?
- 8.10. Werden virtuelle private Netzverbindungen benutzt, um sichere Kommunikationen mit Partnernetzen zu liefern?
- 8.11. Sind Sicherheitsvoraussetzungen für unverschlüsselten Netzverbindungen zu Außenpartnernetzen gegründet worden?
- 8.12. Wenn verdrahtet oder drahtlose Voice over IP (VoIP) für sehr empfindliche Kommunikationen verwendet wird, ist die Übertragung verschlüsselt?

Netzwerk Element Integrität

- 8.13. Ist jeder Router, Schalter, Server, Arbeitsstation, oder andere Informationsausrüstung erfordert minimale Sicherheitsstandards zu entsprechen, bevor es mit dem Netz verbunden wird?
- 8.14. Werden Netzsoftwarebestandteile beim Startup automatisch geprüft für Änderungen in Sicherheitskonfigurationen die gemacht worden sind, seitdem das System letztesmal angefangen wurde und, wenn Änderungen gefunden werden, wird der Systemadministrator automatisch benachrichtigt? *
- 8.15. Sind rechtmässige Systeme die die weite Netzkonnektivität nicht benötigen, von den weiteren Netzen weggehalten worden?
- 8.16. Wird das Netz regelmässig für unberechtigte Systeme überprüft?
- 8.17. Wenn software-gegründete Voice over IP Telefone für empfindliche Kommunikationen verwendet werden, sind die Systeme von Stimmensammlern sicher? *
- 8.18. Sind Tests ausgeführt worden, um sicherzustellen, daß kritische Systeme nicht zu leicht offline genommen werden können durch große Datenmengen oder Verkehr, sowie es in einem Dienstverweigerungsangriff verwendet werden könnte?
- 8.19. Gibt es einen Mechanismen, der kritische Bestandteile wie Webserveranwendungen automatisch wiederanfängt, wann auch immer andere Anwendungen wiederholt

- nicht fähig sind mit denen in Verbindung zu stehen und den Computersystemoperateur zu informieren, daß das getan wurde?
- 8.20. Verwenden kritische Systeme überflüssiges Domain Name System (DNS) Server, um die Wirkung von Unterbrechungen dieses Dienstes von einer Quelle zu vermindern?
 - 8.21. Werden Maßnahmen gebracht, um Domain Name System (DNS) Server für Angriffe zu kontrollieren, die Anforderungen zu unberechtigten Positionen umleiten?
 - 8.22. Sind Verwundbarkeitsscans oder Penetrationstests an kritischen Systemen durchgeführt, bevor die mit den korporativen Netzen verbunden werden?
 - 8.23. Sind Verwundbarkeitsscans oder Penetrationstests regelmäßig an kritischen Systemen innerhalb der korporativen Netze durchgeführt?
 - 8.24. Sind Verwundbarkeitsscans oder Penetrationstests durchgeführt an allen Interneteinfassungen oder Kundeneinfassungssystemen und Anwendungen, bevor die ins Netzwerk platziert werden?
 - 8.25. Sind Verwundbarkeitsscans oder Penetrationstests regelmäßig durchgeführt an allen Interneteinfassungen oder Kundeneinfassungssystemen und Anwendungen die mit dem Netzwerk verbunden werden?

Drahtlose Verbindungen und Modems

- 8.26. Gibt es klare und strikt erzwungene Regeln, für die Errichtung und Benutzung von drahtlosen Verbindungen zu den inneren Netzwerken?
- 8.27. Wird ein drahtloser Analysator periodisch gelaufen, um alle unberechtigten drahtlose Geräte zu identifizieren die vielleicht mit dem Netzwerk verbunden wurden?
- 8.28. Werden infrarote Bluetooth, und drahtlose Verbindungen auf Druckern unbrauchbar gemacht wenn nicht erforderlich für Geschäftsfunktionen?
- 8.29. Wenn eine drahtlose Technologie, wie ein drahtloses lokales Zugriffsnetzwerk (LAN), Bluetooth, oder drahtloser USB, für die empfindlichen Informationen verwendet wird; werden die zur Verfügung gestellten Verbindungen starke Verschlüsselungstechnologien anwenden?
- 8.30. Sind die Persönlichen Identifikationsnummern (PIN) für Bluetooth Geräte geändert, bevor die in Dienst gestellt werden?
- 8.31. Wenn drahtlose Technologie für ein empfindliches Netzwerk verwendet wird, ist das Warnsignal das die Anwesenheit des Netzwerks überträgt, behindert?
- 8.32. Wenn drahtlose Netzwerktechnologie verwendet wird, werden die gemeinsam benutzten Verschlüsselungsschlüssel regelmäßig rotiert?

- 8.33. Wenn drahtlose Netzwerktechnologie verwendet wird, ist Zugang zu den drahtlosen Verbindungen beschränkt zu autorisierten Geräten?
- 8.34. Beauftragen korporative Richtlinien Verfahren, für die Einsetzung von Modems innerhalb der korporativen Infrastruktur?
- 8.35. Sind autorisierte Modems zugegriffen, mit der Verwendung von Sicherheitsmaßnahmen, wie Rückruf und Anrufnachsendungsentdeckungen?
- 8.36. Werden innere war-dialing Kampagnen regelmäßig ausgeführt, um unberechtigte Modems zu identifizieren die mit Einwählungen erreicht werden können?
- 8.37. Wird korporativer Telefonaustausch regelmäßig überprüft, um Außenversuche für die Suche von nicht bevollmächtigten Modems zu entdecken, mit war-dialing Kampagnen ?

Brandschutzmauern und Intrusion Entdeckung und Verhinderungssysteme

- 8.38. Hat die Gesellschaft Listen für die Verkehrsbestimmungsörter und den verschiedenen Verkehr gemacht, sowohl inbound als auch auslaufend, den es durch die Brandmauern erlauben will?
- 8.39. Hat die Gesellschaft ihre Brandmauern konfiguriert, um nur den Verkehr auf ihren genehmigten Listen zu erlauben?
- 8.40. Hat die Vereinigung einen Genehmigungsprozess für alle Änderungen in den Regel-Sätzen um den Verkehr der durch die Brandmauern erlaubt wird zu definieren?
- 8.41. Verlangt die Vereinigung das die Listen des Verkehrs der durch Ihre Brandmauern erlaubt ist, regelmäßig nachgeprüft werden, sodaß die Änderungen in den Verkehrsbedürfnissen der Vereinigung in Betracht gezogen werden können?
- 8.42. Verlangt die Vereinigung periodische Kontrollen der Brandmauern um nachzuprüfen daß die Regel-Sätze ohne Ad-Hoc-Änderungen genau durchgeführt worden sind?
- 8.43. Sind Sicherheitslogs für Brandmauern in einem Weg aufrechterhalten der die davon abhält, modifiziert oder gelöscht zu werden?
- 8.44. Werden Sicherheitslogs für Brandmauern regelmässig nachgeprüft für unberechtigten Verkehr?
- 8.45. Sind da Brandmauern eingesetzt, um kritische Systeme vor dem unberechtigten Zugang vom inneren Personal zu schützen?
- 8.46. Erhält die Gesellschaft umfassende Zugriffsberechtigungslisten für ihre Router einschließlich der Internetprotokolladressen und Port Nummern die benutzt werden, aufrecht?

- 8.47. Verlangt die Vereinigung periodische Kontrollen für ihre Router um nachzuprüfen dass die Zugriffsberechtigungslisten genau durchgeführt worden sind?
- 8.48. Verlangt die Vereinigung, daß die Zugriffsberechtigungslisten für ihre Router regelmäßig nachgeprüft werden, sodaß die Änderungen in den Verkehrsbedürfnissen der Vereinigung in Betracht gezogen werden können?
- 8.49. Werden Intrusion Entdeckungs- und/oder Intrusion Verhinderungssysteme im Netzwerk verwendet?
- 8.50. Sind Sicherheitsalarmsignale von Intrusionentdeckungssystemen dauernd kontrolliert?
- 8.51. Werden Unterschriften auf Intrusion- und Intrusionverhinderungssysteme regelmäßig aktualisiert?
- 8.52. Sind Sicherheitslogs für Intrusionentdeckungssysteme und Intrusionverhinderungssysteme regelmässig nachgeprüft für abnormale Tätigkeitsmuster?
- 8.53. Sind Sicherheitslogs für die Intrusionentdeckung- und Intrusionverhinderungssysteme aufrechterhalten sodaß die nicht modifiziert oder gelöscht werden?

Die Filterung

- 8.54. Werden Webfilter verwendet, um vertrauliche Informationen davon einzuschränken auf web-basierte E-Mail-Anwendungen geladen zu werden? *
- 8.55. Werden Webfilter verwendet, um das Hochladen der empfindlichen Informationen zum Online Speicherungsportal und zum Kontaktverzeichnisportal zu begrenzen?*
- 8.56. Werden Webfilter verwendet, um die Übertragung der empfindlichen Information durch die elektronischen Grußkartenportals einzuschränken? *
- 8.57. Filtert die Gesellschaft Internetdownloads von Angestellten heraus, beruhend auf ihre Arbeitsrollen? *
- 8.58. Verwendet die Gesellschaft Inhaltfilterung um feindliche Aktive X, JavaScript, und Java Applets zu kontrollieren?
- 8.59. Führt die Gesellschaft die Inhaltfilterung auf allen Dateiattachments durch, die durch die E-Mail gesandt werden sodaß Übertragung der empfindlichen Information entweder blockiert oder verfolgt wird? *
- 8.60. Filtert die Gesellschaft alle ausführbaren E-Mail Attachments heraus?
- 8.61. Werden E-Mail-Filter verwendet, um vertrauliche Information davon einzuschränken, zu Außenparteien übergesendet zu werden, wenn nicht autorisiert, und verschlüsselt? *

- 8.62. Verwendet die Gesellschaft Inhaltfilterung, um Instant Messages (IM) die vielleicht empfindliche Informationen enthalten, zu kontrollieren? *
- 8.63. Bezeichnet die Gesellschaft empfindliche Dokumente mit Digitalwasserzeichen sodaß Inhaltfilterung die leichter identifizieren kann?*
- 8.64. Führt die Organisation Inhaltfilterung auf dem Ausgangsdateiübertragungsprotokoll (FTP) oder triviales Dateiübertragungsprotokoll (TFTP) Übertragungen durch, so dass Übertragung der empfindlichen Informationen entweder blockiert oder verfolgt wird?*
- 8.65. Schränkt die Gesellschaft Simple Network Management Protocol (SNMP) Anfragen am Internetgateway ein?
- 8.66. Schränkt die Gesellschaft innere SNMP Anfragen von unberechtigten Systemen zu kritische Server und Netzwerkgeräte ein?
- 8.67. Verwendet die Gesellschaft Eingangs- und Ausgangsfilterung, an den Internetgateways?
- 8.68. Verwendet die Gesellschaft Eingangs- und Ausgangsfilterung an Eingrenzungsroutern, um Personifikation mit spoofed IP Adressen zu verhindern?
- 8.69. Verwendet die Gesellschaft Eingangs- und Ausgangsfilterung, zwischen Partnernetzwerkverbindungen?
- 8.70. Verhindern Brandmauer- oder Routerregeln unberechtigte Ausgangsverbindungen von öffentlichen Belagsystemen wie Webserver?

Allee 9: Zwischenzeitliche Netzwerkverbindungen

Fernmeldeverbindungsprobleme

- 9.01. Benutzen Angestellte, die von Zuhause arbeiten, Computers mit den Brandmauern, Virus-Schutz, Sicherheitspatches, virtuelle private Netzsoftware, und anderer Sicherheiten, die die Gesellschaft als geeignet erachtet?
- 9.02. Wird Angestellten auf der Reise standardisierte Computerausrüstung gegeben, die Sicherheitsmaßnahmen integrieren, um empfindliche Daten zu schützen falls der Computer verloren geht oder gestohlen wird, zusätzlich zu den anderen korporativen Sicherheiten?
- 9.03. Definieren korporative Richtlinien Sicherheitsvoraussetzungen für Einwahlverbindungen zum korporativen Netzwerk oder zum virtuellen privaten Netzwerk?
- 9.04. Definieren korporative Richtlinien Sicherheitsvoraussetzungen für ausserhalb des Geländes befindlichen drahtlose Modems und drahtlose Breitbandverbindungen?
- 9.05. Verwenden telecommuters zwei-Faktor Beglaubigung, um auf das korporative Netzwerk zuzugreifen?

- 9.06. Wird es von telecommuters verlangt, virtuelle private Netzwerkverbindungen zu verwenden, um Zugang zum korporativen Netz zu erhalten?
- 9.07. Wenn ein webbased virtuelles privates Netzwerk verwendet wird, entfernt es Informationen von der Sitzung von dem Computer der die Sitzung begann?
- 9.08. Gibt es Extraüberwachung für entfernte Verbindungstätigkeiten, um auszugleichen daß die in anderer Hinsicht weniger beaufsichtigt werden?

Unregelmäßige Verbindungen durch Angestellte und Partner

- 9.09. Gibt es strikte Kontrollen für alle Laptops, Speicherungsmedien, oder anderen Ausrüstungen die manchmal ins Netz eingesteckt werden, um Wartungsarbeit durchzuführen?
- 9.10. Gibt es strikte Kontrollen für alle Laptops, Speicherungsmedien, oder anderen Ausrüstungen die manchmal ins Netz eingesteckt werden, um Software zu aktualisieren?
- 9.11. Werden infrarote Bluetooth und drahtlose Verbindungen auf Laptops und transportierbaren Digitalhelfern unbrauchbar gemacht wenn nicht erforderlich für Geschäftsfunktionen?
- 9.12. Werden innere Mikrofone und Kameras auf Laptops unbrauchbar gemacht innerhalb empfindlichen Gebieten?
- 9.13. Wenn empfindliche Informationen auf Laptops gespeichert werden müssen, sind diese Informationen verschlüsselt?
- 9.14. Scannt die Vereinigung alle Laptops die mit dem korporativen Netzwerk bei Außenverkäufern und Auftragnehmern provisorisch verbunden werden, um nachzuprüfen, daß die frei von Viren, Würmern, und andere malware sind?
- 9.15. Werden die Tätigkeiten die bei Laptops ausgeführt werden, die mit dem korporativen Netzwerk bei Außenverkäufern und Auftragnehmern provisorisch verbunden werden, verfolgt?
- 9.16. Definieren korporative Richtlinien Sicherheitsvoraussetzungen für transportierbare Digitalhelfer, Smart Phones, USB Drives, iPods, Digitalkameras, und andere Geräte die mit dem korporativen Netzwerk verbunden werden können?
- 9.17. Falls entfernbare Informationsgeräte erlaubt sind, kontrolliert die Organisation den Gebrauch solcher Geräte? *
- 9.18. Falls transportierbare Digitalhelfer oder Smart Phones erlaubt sind, beeinschränkt die Organisation die Herunterladung von empfindlichen Informationen auf diese Geräte?

- 9.19. Wenn empfindliche Informationen auf transportierbaren Digital Helfern oder Smart Phones provisorisch gespeichert werden müssen, sind diese Informationen verschlüsselt?
- 9.20. Falls transportierbare Digital Helfer oder Smart Phones erlaubt sind, werden Antivirus-Anwendungen auf diesen Geräten installiert?
- 9.21. Wenn Antivirus-Software auf transportierbare Digital Helfer oder Smart Phones verwendet wird, werden die Definitionsdateien regelmäßig aktualisiert?

Verbindungen des Elektronischen Handels

- 9.22. Wenn Geschäftstransaktionen über das Internet ausgeführt werden, werden Daten vom Kunden und vom Computer des Kunden gesammelt der helfen wird die Transaktion zu beglaubigen?
- 9.23. Gibt es einen Mechanismus der erlaubt Kunden nachzuprüfen, dass sie auf einer legitimen Website der Gesellschaft sind, mit welcher sie vorhaben, Geschäfte zu machen? *
- 9.24. Sind Kundenüberprüfung für Transaktionen des elektronischen Handels geschützt vor automatisierten Angriffen durch die Anzeige eines Bildes oder Audioplay-Backs das ein Muster enthält welches nur von einem Menschen anerkannt werden kann? *
- 9.25. Wenn Internetgeschäftstransaktionen finanziell groß genug sind, werden diese Transaktionen durch Digitalzertifikate, zwei-Faktor Tokens, oder zusätzliche Beglaubigungsmechanismen beglaubigt?
- 9.26. Wenn Digitalzertifikate für Transaktionen des elektronischen Handels verwendet werden, werden diese Zertifikate von einer Industrie genehmigten Zertifikatautorität ausgegeben?
- 9.27. Wenn Digitalzertifikate für Transaktionen des elektronischen Handels verwendet werden, gibt es einen Mechanismus, um nachzuprüfen, daß die Angelegenheit wirklich von dem System geführt wird für welches das Zertifikat ausgegeben wurde?*
- 9.28. Gibt es Mechanismen die gegründet wurden, um die Modifizierung der Ordnungen oder Instruktionen für über das Internet geführten Geschäftstransaktionen zu verhindern?
- 9.29. Gibt es einen Mechanismus der eine Sitzung des elektronischen Handels nach einem Zeitraum der Untätigkeit automatisch begrenzen wird?
- 9.30. Werden empfindliche Kundeninformationen, wie Kreditkartennummern und persönliche Identifizierungen, bei anderen Systemen gehandelt anders als das System das die Webtransaktion selbst behandelt?

- 9.31. Werden Kundenwebsites mit der Antifälschungssoftware ausgestattet, die, wenn ein Versuch gemacht wird die zu verunstalten, automatisch jede Seite zu ihrer richtigen Bedingung wiederherstellt?
- 9.32. Werden Webportals für den elektronischen Handel öfter für Sicherheitsprobleme überprüft als andere korporative Informationssysteme?

Allee 10: Netzwerkwartung

Netzwerkdokumentation

- 10.01. Gibt es ausführliche Netzwerktopologiediagramme von dem korporativen Netzwerk, sodaß allen Verbindungswegen nachgespürt werden kann?
- 10.02. Falls es diese Netzwerktopologiediagramme gibt, werden die Dienstwege und Protokolle, die verwendet wurden, gelistet?
- 10.03. Wurden die Informationen für das Netzwerktopologiediagramm nachgeprüft, um sicherzustellen das die fehlerfrei sind, sodaß alle Bestandteile und Verbindungen im Netzwerk tatsächlich eingeschlossen wurden?
- 10.04. Gibt es einen Grundriss oder geographische Karte die genau zeigt wo die Netzwirkabel gelegt worden sind?
- 10.05. Werden alle Dokumente die Netzwerktopologies und physische Entwürfe schematisieren, vor dem unberechtigten Zugang gründlich geschützt?
- 10.06. Wurden alle Kabel und Ausrüstung physisch etikettiert in den Verteilerschränken und in anderen Plätzen wo die vielleicht wiederkonfiguriert werden müssen?
- 10.07. Gibt es Etiketten für die Ausrüstung auf beiden der Vorderseite und Rückseite der Ausrüstungshülle, um die Gefahr zu reduzieren das die Ausrüstung unpassend wiederkonfiguriert wird?

Sicherheitsrichtlinien und Standards

- 10.08. Gibt es ein System, um Softwarepatches und Aktualisierungen zu verfolgen, das loggt die Neuigkeiten das die benötigt werden, das bekanntgegebenen Ausgabedatum, und die Daten wenn die wirklich erhalten worden sind?
- 10.09. Werden die relevanten Leute innerhalb der Organization gewarnt zu allen neuen Verwundbarkeiten, sodaß sie Ersetzende- und Schutzmaßnahmen ergreifen können, um die Periode zwischen der Zeit der Entdeckung dieser Verwundbarkeiten und der Zeit ein relevanter Patch oder Aktualisierung installiert wird, zu umfassen?
- 10.10. Gibt es Verfahren, um Softwarepatches und Aktualisierungen durchzuführen, um die Gefahren von Funktionsstörungen von der vorherigen Prüfung zu minimieren, sowie vorsichtig gewählte Installierungszeiten, und Notverfahren, um schnell zum letzten bekannten guten Zustand zurückzukehren?

- 10.11. Werden Sicherheitseinstellungen und Konfigurationen wiederüberprüft, nachdem Patches und Aktualisierungen installiert worden sind, um sicherzustellen, daß die nicht unachtsamerweise zu weniger sicher oder Standardeinstellungen zurückgesetzt worden sind?
- 10.12. Gibt es ein regelmäßiges Verfahren, um nachzuprüfen, daß die Softwarepatches und Aktualisierungen die verfolgt wurden, tatsächlich auf eine rechtzeitige und regelmäßige Weise installiert wurden?
- 10.13. Werden Lieferanten Standardsicherheitseinstellungen auf Systemen geändert, bevor diese Systeme auf das Netzwerk gelegt werden?
- 10.14. Gibt es Richtlinien, für die Begrenzung und Überwachung des Gebrauchs von entfernten Verwaltungswerkzeugen die es erlauben würden die Systeme von ausserhalb des korporativen Netzwerks zu kontrollieren?
- 10.15. Hat die Organisation Abmachungen mit Verkäufern, in welchen sie ein angegebenes Niveau der Netzzuverlässigkeit und des Dienstes versichern?
- 10.16. Gibt es Verfahren für die Ratenbeschränkung des Verkehrs, sodaß das Netzwerk durch übermäßige Lasten auf den betroffenen Dienstleistungen nicht untauglich gemacht wird?
- 10.17. Gibt es Verfahren, um zusätzliche Server hinzuzufügen und Verkehr umzuadressieren, um kritische Netzbestandteile davon abzuhalten, durch übermäßige Lasten auf den betroffenen Dienstleistungen untauglich gemacht zu werden?
- 10.18. Verboten korporative Richtlinien den Gebrauch von unverschlüsselten Protokollen, wie Telnet, FTP, und SNMP für die Systemverwaltung, solange wie das System diese Protokolle nicht verlangt?
- 10.19. Falls die Systeme unverschlüsselte Protokolle für ihre Verwaltung verlangen, werden die entsprechenden Verbindungen gesetzt, um nach einer beschränkten Zeitspanne abzuschalten?
- 10.20. Sind alle Server und Arbeitsstationen zu einem angegebenen Sicherheitsstandard konfiguriert?
- 10.21. Sind alle Netzbestandteile, wie Router und Schalter, konfiguriert zu einem angegebenen Sicherheitsstandard?
- 10.22. Sind alle Brandmauern und Intrusionentdeckungssysteme zu einem angegebenen Sicherheitsstandard konfiguriert?
- 10.23. Ist das entfernte Management von Routern, Schaltern, und anderen Netzbestandteilen nur auf autorisierte Internetprotokolladressen eingeschränkt?

- 10.24. Ist logischer Zugang zu den Verwaltungsschnittstellen von Sicherheitsbestandteilen (z.B. Brandmauer, IDS, usw.) nur auf autorisierte Systeme oder Internetprotokolladressen eingeschränkt?

System und die Sicherheitsprotokollierung

- 10.25. Werden Konfigurationsmodifizierungen zu allen kritischen Servern protokolliert?
10.26. Werden Konfigurationsmodifizierungen zu Routern und Schaltern protokolliert?
10.27. Werden Konfigurationsmodifizierungen zu Brandmauern und Intrusionentdeckungssystemen protokolliert?
10.28. Wird syslog auf kritischen Servern eingeschaltet und werden die Informationen in ein entferntes System geloggt?
10.29. Wird syslog auf Routern und Schaltern eingeschaltet und werden die Informationen in ein entferntes System geloggt?
10.30. Wird syslog auf die drahtlosen Zugriffspunkte eingeschaltet und werden die Informationen in ein entferntes System geloggt?

Gebiet Vier: Automationsverwundbarkeiten

Allee 11: Entfernte Sensoren und Regelsysteme

- 11.01. Gibt es eine gesamte Karte die genau alle Kommunikationswege, durch welche Regelsysteme verbunden werden, identifiziert?
11.02. Entwerfen alle Dokumente die logischen Zugriffswege um Systeme die gründlich vom unberechtigten Zugang geschützt sind zu kontrollieren?
11.03. Sind alle Regelsysteme die nicht mit dem Internet verbunden werden müssen, isoliert von dem Internet?
11.04. Werden alle Verbindungen zwischen Regelsystemen und dem Internet, regelmäßig bewertet, um zu sehen, ob die wirklich notwendig sind?
11.05. Werden alle Regelsysteme vom korporativen Netzwerk isoliert, wann auch immer es keinen zwingenden Grund gibt, die zu verbinden?
11.06. Wenn ein Regelsystem vom korporativen Netzwerk nicht isoliert werden kann, wird das Regelsystem durch hoch einschränkende Brandmauern und Intrusionentdeckungssystemen geschützt?
11.07. Wurde Acht gegeben daß Einbrecher nicht mit deutlich etikettierten schematischen Diagrammen der physischen Prozesse und der Systeme die die verwalten, präsentiert werden?

- 11.08. Wurden die Adressen- und Befehlscodes für Regelsystemsbestandteile, wie entfernt bediente Schalter und Ventile, zugeteilt oder wiederzugeteilt auf solche Art und Weise daß die nicht zu leicht zu erraten oder abzuleiten sind? *
- 11.09. Gibt es Bestimmungen wie entfernte Warnungen, die warnen würden, wenn die entfernten Sensoren vor Ort physisch manipuliert werden, um falsche Lesungen zu erzeugen?
- 11.10. Wurden die entfernten Sensoren entworfen oder modifiziert um es schwierig zu machen, die Sensoren zu veranlassen falsche Daten zu melden, wenn die physisch manipuliert werden? *
- 11.11. Sind sehr kritische Kontrollen durch einen zweiten Kontrollkanal zugänglich, sodaß auf die noch zugegriffen werden kann, wenn der erste Kanal versagt?
- 11.12. Gibt es die zweiten Sätze von Sensoren die kritische Prozesse mit einer verschiedenen Messtechnik kontrollieren, sodaß eine falsche Lesung vom ersten Satz von Sensoren schnell entdeckt werden kann? *
- 11.13. Wenn entfernte Sensoren über Cellular, Satelliten oder andere drahtlose Verbindungen kommunizieren, wurden Maßnahmen genommen um die Fälschung von Informationsübertragungen zu verhindern? *
- 11.14. Gibt es Pläne und Verfahren, um sich mit kritischen drahtlosen Verbindungen die blockiert worden sind, zu befassen?
- 11.15. Falls entfernte Datenstationseinheiten die Fähigkeit haben, Kennwörter oder Verschlüsselung zu verwenden, und die betrieblichen Geschwindigkeitsvoraussetzungen es erlaubt, werden diese Sicherheitsmaßnahmen verwendet?
- 11.16. Haben alle neuen entfernten Datenstationseinheiten und andere Kontrolgeräte, die im Netzwerk installiert werden, veränderliche Kennwörter oder andere wiederprogrammierbare Beglaubigungsmechanismen?
- 11.17. Sind alle periodisch automatisierten Übertragungen von kritischen Kontrolldaten, wo Geschwindigkeit nicht ein Problem ist, durch die Verschlüsselung geschützt?
- 11.18. Werden kritische Systemsbestandteile konfiguriert, um ihre Zeit von einer sicheren Zeitquelle regelmäßig zu aktualisieren?
- 11.19. Sind alle Bestandteile innerhalb des synchronisierten Netzwerks, sodaß die dieselbe Zeit, Zeitzone, und Datum verwenden?
- 11.20. Aktualisieren besonders kritische Systemsbestandteile ihre Zeit von verschiedenen Zeitquellen regelmäßig, sodaß spoofing oder Korruption der Kommunikationen mit einer Zeitquelle entdeckt werden kann? *

- 11.21. Sind da genügend Warnungen um Bediener zu warnen, wenn irgendwelche kritischen Prozesse in der Gefahr sind, sich außerhalb des normalen Parameters der sicheren Operation zu bewegen? *
- 11.22. Werden Aktualisierungen zu den Betriebssystemen von entfernten Datenstationseinheiten in einer sicheren Weise von einer sicheren Quelle gesendet?
- 11.23. Werden Statusfragen zu entfernten Datenstationseinheiten in einer sicheren Weise von einer sicheren Quelle gesendet?

Allee 12: Backup Verfahren

Backup Strategie

- 12.01. Sind die Betriebssysteme, Programme, und Betriebsinformationen gesichert, sowie die Daten?
- 12.02. Werden die Daten passend zu deren Wirtschaftswert und dem Tempo in welchem die geändert werden, häufig gesichert?
- 12.03. Werden die Backup Daten lange genug gespeichert, sodaß es noch eine unverdorben Kopie geben würde, falls die Daten auf eine "schwierig-zu-entdecken" Weise schrittweise verdorben würden über einen langen Zeitraum?
- 12.04. Werden alle Tätigkeitlogs die Sicherheitsrelevant sein könnten oft gesichert und in einer Form gespeichert die herumpfuschen verhindern würde?
- 12.05. Werden die Konfigurationen von Schaltern und Routern regelmäßig gesichert?
- 12.06. Werden die Protokolldateien für Anwendungszugang regelmässig zu einen sicheren Platz gesichert?
- 12.07. Werden die Protokolldateien für Anwendungszugang lang genug gehalten sodaß alle Quellen für allmähliche Datenkorruption verfolgt werden könnten?
- 12.08. Gibt es vielfache Backups, sodaß wenn eins verloren oder verdorben wird, könnte das System doch noch wiederhergestellt werden?
- 12.09. Werden die Backups regelmäßig geprüft, um sicherzustellen, das die lesbar und unverdorben sind?
- 12.10. Gibt es Verfahren, um sich mit Backup Daten die verdorben worden sind zu befassen, besonders während einer Krise? *
- 12.11. Wird der Backup regelmäßig zu einem Speicherungsgerät das vom Netzwerk isoliert ist, übertragen?
- 12.12. Wird der Backup regelmäßig zu einer physisch entfernten Stelle übertragen?
- 12.13. Werden kritische Backups, die noch nicht zu einer entfernten Stelle übertragen worden sind, gespeichert und etikettiert auf einer Art und Weise sodaß die leicht mitgenommen werden könnten im Falle einer Evakuierung?

12.14. Wenn der Verlust der gesicherten Informationen das Unternehmen gefährden würde, gibt es Backups an mehr als einer entfernten Stelle?

Backup Sicherheit

12.15. Gibt es Verfahren, um sich mit dem Verlust oder Diebstahl von unverschlüsselten Backupbändern, die empfindliche oder Eigentumsinformationen enthalten, zu befassen?

12.16. Schließt das Backupverfahren die Überprüfung der Daten für den feindlichen Code wie Viren und trojanische Pferde bevor der Sicherung der Informationen ein? *

12.17. Wenn die Informationen, die gesichert werden, empfindlich oder eigentümlich sind, sind die Informationen verschlüsselt während des Sicherungsprozesses, sodaß es in einer verschlüsselten Form gespeichert wird? *

12.18. Werden alle Verschlüsselungsschlüssel die im Backup benutzt werden, in einer sicheren Stelle aufbewahrt und rotiert um sicherzustellen das der eine kompromittierte Schlüssel nicht alle Daten aufdeckt? *

12.19. Werden die Verschlüsselungsschlüssel für die Backups zusammen mit einer Liste für wenn und wo die benutzt wurden, in einem anderen Platz, in einer sicheren Form aufbewahrt? *

12.20. Wenn die Backupkopien physisch zu einem entfernten Ort transportiert werden, werden die in einbruchssichere Behälter gesetzt, sicher transportiert und auf dem Transportweg verfolgt? *

12.21. Sind alle Backupmedien geschützt vor dem physischen Diebstahl während der Lagerung, egal ob die lokal oder entfernt gelagert werden?

12.22. Wenn die Backuplagerungsmedien nicht mehr für Backups benötigt werden, gibt es da sichere Verfahren, um diese Medien zu zerstreuen oder wiederzuverwenden, egal ob die lokal oder entfernt gelagert werden?

12.23. Wenn die Backup Kopie elektronisch zu einem entfernten System gesendet wird, wird die Information dieser Stelle durch verschlüsselte Mittel oder über ein geeignetes sicheres Netzwerk übertragen?

Gebiet Fünf: Human Bedienerverwundbarkeiten

Allee 13: Human Wartung von Sicherheitsverfahren

Sicherheitsausbildung

13.01. Wird allen Angestellten periodische Ausbildung für die Sicherheitsrichtlinien gegeben die für das Geschäft wichtig sind, mit genügend Erklärungen, warum diese Richtlinien wichtig sind?

- 13.02. Werden Angestellte geschult um ihre laptops und andere transportierbare Informationsausrüstung unter der Bewachung zu haben oder in sicheren Plätzen zu behalten, wenn die außerhalb des Arbeitsplatzes getragen oder benutzt werden?
- 13.03. Werden Angestellte geschult nicht Kennwörter die aus persönlichen biographischenTatsachen gebaut wurden, zu wählen, da diese vielleicht öffentlich zugänglich sind?
- 13.04. Werden Angestellte auf die Gefahren für unsichere Kennwortspeicherung hingewiesen, wie zum Beispiel wenn sie das Kennwort auf einen Zettel schreiben und in dem Arbeitsplatz hinterlassen?
- 13.05. Werden Angestellte unterrichtet welche Sorte von den durch die Gesellschaft behandelten Informationen, als empfindliche Informationen betrachtet werden sollen?
- 13.06. Werden Angestellte unterrichtet, um gegen alle Software die in der Post kommt mißtrauisch zu sein, wenn es auch erscheinen kann das die paketiert und von vertrauten Verkäufern gesendet wurden?
- 13.07. Sind die Angestellten unterrichtet worden, nicht Opfer zu sozialen Manipulationen telefonisch oder über das Internet zu fallen die sie dazu bringen würde private Informationen zu offenbaren oder spezifische Folgen von Zahlen oder Buchstaben zu wählen oder zu tippen?
- 13.08. Werden Angestellte regelmäßig erinnert Dateien nicht herunterzuladen, die ausführbare Codes enthalten könnten, misstrauische E-Mails nicht zu öffnen, und persönliche Software auf korporativen Systemen nicht zu installieren?
- 13.09. Werden Angestellte auf die Sicherheitsrisikos aufmerksam gemacht, die sie sich zuziehen können, indem sie persönliche Informationen, besonders persönliche Identifizierungsinformationen auf ihren Mobiltelefonen speichern?
- 13.10. Sind Angestellte von der Tatsache zur Kenntnis gebracht worden, das massenhaft erzeugte und verteilte Software noch gezielte malware enthalten könnte?
- 13.11. Werden Angestellte unterrichtet, wie gefährlich es ist Netzwerkverbindungen zu installieren, die undokumentiert und vom Sicherheitspersonal nicht autorisiert wurden, sogar wenn diese Verbindungen von Leitenden Angestellten angefordert wurde?
- 13.12. Werden alle Angestellten auf ihren Kenntnissen von Sicherheitsverfahren einschließlich ihrer Kenntnisse kürzlich erscheinender Drohungen regelmäßig geprüft?

Sicherheitsverantwortlichkeit

- 13.13. Ist das Aufrechterhalten der Sicherheit der Gesellschaft ein Teil der Jobbeschreibung jedes Angestellten?
- 13.14. Sind alle Außenauftragnehmer, Gebäudebetriebsleiter, Boten, und Wartungsgesellschaften ausführlich informiert über die korporativen Sicherheitsrichtlinien und Standards die für ihre Tätigkeiten gelten?
- 13.15. Sind alle Außenauftragnehmer, Gebäudebetriebsleiter, Boten, und Wartungsgesellschaften ausführlich informiert über die korporativen Sicherheitsrichtlinien und Standards die für ihre Tätigkeiten gelten?
- 13.16. Sind alle Außenauftragnehmer, Möglichkeitsbetriebsleiter, Boten, und Wartungsgesellschaften vertraglich dazu verpflichtet, Sicherheitsrichtlinien und Standards mindestens ebenso strikt aufrechtzuerhalten, wie die Gesellschaft selbst die aufrechterhält?
- 13.17. Werden gesetzliche Benachrichtigungen auf den Anmeldungs und Beglaubigungsbildschirmen angeschlagen, warnend, das unberechtigter Zugang oder Gebrauch ein ungesetzliches Eindringen darstellt?
- 13.18. Wird Angestellten verboten, irgendwelche Software auf korporativen Maschinen zu installieren die persönlich, für Freizeit, oder einfach nicht bevollmächtigt ist?
- 13.19. Definieren korporative Richtlinien den richtigen Gebrauch der E-Mails, des Internetzugangs, und der sofortigen Nachrichtenübermittlung durch Angestellte?
- 13.20. Wird Angestellten verboten, andere Angestellte ihre Personalcomputer benutzen zu lassen?
- 13.21. Wird Angestellten verboten, Kennwörter zu teilen?
- 13.22. Wird Angestellten verboten, persönliche Identifizierungsgeräte, wie Abzeichen und Nähe-Karten zu verwenden, um anderen Mitarbeitern Zugang zu Informationen und Systemen zu geben?
- 13.23. Ist jede Informationsausrüstung die die Vereinigung besitzt oder pachtet die ausführliche Verantwortung eines bestimmten Angestellten?
- 13.24. Ist der Angestellte der für eine gegebene Informationsausrüstung verantwortlich ist, erfordert die allgemeine Sicherheit dieser Ausrüstung zu beaufsichtigen?
- 13.25. Gibt es dauerhafte Schilder oder andere sich identifizierende Markierungen die es leicht machen für andere Angestellte zu bestimmen, wer eine gegebene Informationsausrüstung "besitzt"?
- 13.26. Wird Angestellten entsprechenden Ansporn gegeben, Sicherheitsbrüche und schlechte Sicherheitspraxen zu berichten, während sie gleichzeitig von irgendwelcher Schuld isoliert werden?

13.27. Werden Angestellte strikt verantwortlich gehalten für alle Handlungen, die sie auf dem korporativen Informationssystem ausführen die in der Übertretung von korporativen Sicherheitspolicen sind?

Sicherheitsbewertungen

13.28. Werden die Informationssicherheitspolicen der Vereinigung und ihre Erfüllung jährlich nachgeprüft bei einem erfahrenen Außenrechnungsprüfer?

13.29. Ist die jährliche Bewertung der Informationssicherheitspolicen der Vereinigung und ihrer Erfüllung großzügig genug in der Reichweite, um Informationsverwundbarkeiten in den physischen Gebäuden und im Mitarbeiterbenehmen aufzudecken?

13.30. Werden die Informationssicherheitspolicen der Vereinigung und ihre Erfüllung, vorsichtig überprüft, um nachzuprüfen, das die Vereinigung mit den Regulierungen und anerkannten Standards für diese Industrie entgegenkommend ist?

13.31. Sind die Rechnungskontrollen und Bewertungen der Informationssicherheit der Vereinigung analytisch untersucht, um Gebiete zu identifizieren, wo verschiedene oder zusätzliche Gegenmaßnahmen erforderlich sein könnten?

13.32. Gibt es ein zuverlässiges System, um die ganzen Verwundbarkeiten, bemerkt von Angestellten, entdeckt durch Rechnungskontrollen, gemeldet von Verkäufern, oder bedeckt in den Medien aufzulisten und zu verfolgen, sodaß Sicherheitspersonal auf eine aktuelle Liste schnell und regelmäßig zugreifen kann, die zeigt, welche Verwundbarkeiten bereits behoben worden sind, und welche noch in Ordnung gebracht werden müssen?

13.33. Werden unterstützende Handlungen ständig auf eine rechtzeitige Weise übernommen, sodaß man sich mit mehr bedeutenden Verwundbarkeiten aufgedeckt oder gemeldet befassen kann?

13.34. Sollen unterstützende Programme die sich mit kürzlich aufgedeckten Verwundbarkeiten befassen auf einer Monatsbasis kontrolliert werden, um sicherzustellen, das es schnellen und unveränderlichen Fortschritt in jenen Gebieten gibt?

13.35. Sind die aufeinander folgenden Rechnungskontrollen und Bewertungen der Informationssicherheit der Vereinigung verglichen, sodaß ältere Betriebsleiter sicherstellen können, das sich die Informationssicherheit der Vereinigung verbessert, anstatt sich zu verschlechtern?

Vorfallbehandlung und Erwidmung

- 13.36. Werden verschiedene Cyberangriffsstrategien in genug Detail und mit genug Variation beschrieben, sodaß die Angestellten eine gute Chance haben würden, die frühen Zeichen solcher Angriffe anzuerkennen und die schnell zu melden?
- 13.37. Wissen Angestellte, wen sie sowohl innerhalb als auch außerhalb der Vereinigung im Falle eines offenbaren Angriffs benachrichtigen sollten?
- 13.38 Sind Angestellte mit dem Zugang zu sehr kritischen Systemen oder Einrichtungen mit speziellen Zugriffscodes versorgt die Signale geben würden, das sie unter Zwang handeln? *
- 13.39 Sind automatisierte Entdeckungssysteme im Platz der stille, entfernte Warnungen erheben würde, wenn die Zwang-Codes verwendet werden? *
- 13.40. Gibt es alternative Kanäle der Kommunikation die benutzt werden können falls normale Kanäle kompromittiert werden?
- 13.41. Wissen Angestellte, wie man die Systeme isoliert die kompromittiert worden sind, bei der Entfernung von dem Netzwerk?
- 13.42. Gibt es Pläne, um Systeme die vielleicht mit falschen Informationen kontaminiert wurden, manuell unter Quarantäne zu stellen und zu kontrollieren ohne die zu schließen?
- 13.43. Gibt es ein Verfahren, um die Quarantänelinien zu bewegen, wenn bessere Informationen über die mögliche Verunreinigung verfügbar wird?
- 13.44. Wissen Angestellte, wie man über die Wiederherstellung von kontaminierten Informationssystemen zu ihrem letzten bekannten guten Zustand geht?
- 13.45. Gibt es einen Mechanismus, um "letzter bekannter guter Zustand" wiederzubekommen, wenn dieser Zustand eine beträchtliche Zeit in der Vergangenheit ist?
- 13.46. Falls es andere Systeme gibt, die mit den geschlossenen oder unzuverlässigen Systemen ausgewechselt werden könnten, wissen Angestellte, wie man auf die umschaltet?
- 13.47. Wissen Angestellte, wo sie sich für die Zusatzinformationen und Leitung während einer ständigen Folge von Angriffen wenden sollten?
- 13.48. Wenn die Vereinigung dringend benötigte Dienstleistungen dem Kundenstamm liefert, gibt es eine geordnete Liste wo Kunden der höchste Vorrang für die Wiederherstellung von Dienstleistungen gegeben wird?
- 13.49. Weiß das Hauptansprechpersonal, wie man die Beweise notwendig für richtige forensische Untersuchungen und gesetzliche Strafverfolgungen sammelt und bewahrt?

- 13.50. Werden Übungen regelmäßig geführt, in welche Schlüsselangestellte die Bewegungen der Reaktion auf einen Kyberangriff auf eine vernünftig realistische Weise durchgehen?
- 13.51. Werden Angestellte erzogen, um Lagerungsmedien und Nebenprodukte sicher in den speziellen durch die Katastrophe-Wiederherstellung erzeugten Verhältnissen zu behandeln?
- 13.52. Ist dem Schlüsselpersonal Gelegenheiten gegeben worden, ihre Notantworten in wirklichen Simulationen zu üben? *
- 13.53. Sind sowohl echte Ereignisse als auch Übungen gefolgt bei Diskussionen der Hinterher-Handlung um zu identifizieren ob die Lehre gelernt wurde?

Allee 14: Absichtliche Handlungen, die Sicherheit Drohen

Werdegangkontrollen

- 14.01. Werden Werdegangkontrollen auf Angestellten mit höheren Niveaus des Informationszugangs ausgeführt, wenn auch ihre Gehälter und Job-Titel dieses Niveau des Zugangs nicht anzeigen können?
- 14.02. Wenn ein Angestellter zu einem beträchtlich höheren Niveau der Verantwortung und des Zugangs befördert wird, wird eine neue Werdegangskontrolle ausgeführt?
- 14.03. Wird eine Werdegangskontrolle ausgeführt für Wartungspersonal wie Portier?
- 14.04. Wenn es eine erkennbare Änderung im persönlichen oder finanziellen Benehmen eines Angestellten mit dem Zugang zu kritischen Systemen gibt, gibt es ein Verfahren, um eine neue Werdegangskontrolle unauffällig auszuführen, solche Dinge wie schnelle Änderungen in der Kreditwürdigkeit oder Zeichen des unerklärten Reichtums bedeckend? *
- 14.05. Wird sich Mühe gegeben, um den gegenwärtigen Verbleib von vorigen Angestellten zu verfolgen die sehr kritische Systeme und Verfahren kannten?

Verhaltenskontrollen

- 14.06. Werden Informationen allgemein überall in der Vereinigung auf einer Basis "wissen müssen" verbreitet, noch das Bedürfnis nach dem kreuz-disziplinarischen Informationsteilen und der Wichtigkeit das die Angestellten die Gründe für was sie tun verstehen?
- 14.07. Wenn eine gegebene Kategorie des Eingangs kritisch genug ist, verlangt die Vereinigung, dass ein zweiter Angestellter die Eingabe nachprüft, bevor die bearbeitet wird?

- 14.08. Werden Gebiete der Verantwortung unter Angestellten auf solche Art und Weise verteilt, das ein einzelner Angestellter eine kritische Operation ohne die Kenntnisse anderer Angestellten nicht ausführen kann?
- 14.09. Beschränkt die Vereinigung Mitarbeiterzugang zu kritischen Systemen von unbeaufsichtigten Lokalen und in unbeaufsichtigten Zeiten?
- 14.10. Werden Gebäudewartungspersonal, wie Portier, gehindert, in sehr empfindliche Gebiete zu gehen, wenn nicht direct beaufsichtigt durch das Sicherheitspersonal?
- 14.11. Wird Videokontrolle für Gebäudewartungspersonal wie Portier sogar in Gebieten ausgeführt die nur gemäßigt empfindlich sind?
- 14.12. Wird der physische und elektronische Zugriffslöcher des Angestellten regelmäßig nachgeprüft um Zugriffsmuster zu identifizieren die durch normale Arbeitsverantwortungen nicht motiviert werden?
- 14.13. Kontrolliert die Vereinigung systematisch für vielfache erfolglose Anmeldeversuche von ihren eigenen Angestellten?
- 14.14. Werden Angestellte gehindert, auf Dateien zuzugreifen die offenbaren würden, wenn ihr Benehmen kontrolliert wird, und ob es spezielle Aufmerksamkeit angezogen hat?
- 14.15 Wird es verlangt das Angestellte periodische Urlaube nehmen, sodaß laufende Tätigkeiten, die sie sonst verbergen könnten, durch ihren vorläufigen Ersatz bemerkt würden?
- 14.16. Gibt es Maßnahmen um Angestellte davon abzuhalten die Geschäftsräume mit den empfindlichen Informationen auf Floppy Discs oder USB Geräte, zu verlassen? *

Mitarbeiterbeziehungen

- 14.17. Macht die Vereinigung Fairness und guten Glauben für die Behandlung von Angestellten einen höheren Vorrang als das Greifen jeder Gelegenheit, einen Kurzzeitwettbewerbsvorteil zu gewinnen?
- 14.18. Stellt die Vereinigung entsprechende Mechanismen für Angestellte zur Verfügung, um ihre Beschwerden ohne Strafe auszudrücken, und um zu sehen das diese Beschwerden gewissenhaft erledigt werden?
- 14.19. Behandelt die Vereinigung Reduzierungen gewissermaßen sodaß feindliche Gefühle seitens voriger Angestellter minimiert werden?
- 14.20. Bietet die Vereinigung ein Verfahren an das Angestellten erlauben würde, Versuche von Außenseitern zu melden die ihre Zusammenarbeit im Überlisten der Sicherheit erpressen, ohne die Basis für diese Erpressung weit zu offenbaren oder einen Teil der dauerhaften Unterlagen dieses Angestellten zu machen?

- 14.21. Wenn ein Angestellter durch eine Periode von großen Schwierigkeiten in seinem oder ihrem persönlichen Leben geht, gibt es eine Politik, um die Verantwortungen dieses Angestellten für kritische Systeme und Zugang zu kritischen Systemen provisorisch zu reduzieren?

Gebiet Sechs: Softwareversorgungsverwundbarkeiten

Allee 15: Innere Policen für die Softwareentwicklung

Sichere Verfahren, um Neue Software zu entwickeln

- 15.01. Hat die Vereinigung eine schriftliche Politik, die über die Schritte und Verfahren für die innere Entwicklung der Software ausführlich berichtet?
- 15.02. Folgt der Softwareentwicklungskreis Richtlinien beruhend auf die Industrie beste Praxen bezüglich der Sicherheit?
- 15.03. Verlangen korporative Sicherheitspolicen, daß alle Verkäufer- und Auftragnehmer-Personal, das an der Softwareentwicklung arbeitet, minimalen Sicherheitsanforderungen entspricht?
- 15.04. Werden die vorgeschlagenen Softwaredesigns von der Einstellung der Informationssicherheit von Sicherheitsfachmännern bewertet, bevor die Alpha-Versionen geschaffen werden?
- 15.05. Hat die Vereinigung ein System, um genau zu verfolgen, welcher Angestellter oder Außenmitwirkender jede Linie des Codes für irgendwelche Software erzeugt intern, schrieb?
- 15.06. Werden alle Programmierer, die an jeder Softwareanwendung arbeiten, bewußt gemacht das Aufzeichnungen von wer jede Linie des Codes schrieb, genau behalten werden?
- 15.07. Hat die Vereinigung Verfahren für die regelmäßige Einfügung des Codes während der Softwareproduktion, sodaß keiner eine Gelegenheit hat, eine Linie des Codes zu verändern, außer dem Programmierer der als verantwortlich registriert wurde? *
- 15.08. Werden Änderungen zur Quellcodebibliothek kontrolliert und überwacht, sodaß die Quellkontrolleinheit von jemandem mit Verwalter-Vorzügen nicht umgangen werden kann? *
- 15.09. Werden Kommentare auf jedem Abteilungscode aufrechterhalten, wie es geschrieben wird, sodaß andere Entwickler und Sicherheitsfachmänner schnell verstehen können, für was eine gegebene Abteilung entworfen wurde?
- 15.10. Hat die Vereinigung vorgenehmigte Codemodule die in die neue Software eingefügt werden können, um Standardsicherheitsfunktionen, wie Beglaubigung und Verschlüsselung zu vollbringen?

- 15.11. Versorgt die Vereinigung Entwickler mit Scheindaten, sodaß die Anwendungen unter Entwicklung nicht auf privaten, empfindlichen oder Eigentumsinformationen erprobt werden müssen?
- 15.12. Werden die Anwendungen unter Entwicklung in Testumfeldern erprobt die von den wirklichen Produktionsumgebungen völlig isoliert werden?

Sicherheitseigenschaften, um in die Neue Software Einzubauen

- 15.13. Wurde die Anwendung entwickelt um empfindliche Informationen zu verschlüsseln, die es in einer Datei oder Datenbank speichert?
- 15.14. Wurde die Anwendung entwickelt um empfindliche Informationen zu verschlüsseln, die es zu der lokalen System-Registrierung schreibt?
- 15.15. Wurde die Anwendung entwickelt um empfindliche Informationen zu verschlüsseln, die es zu dem unbeständigen Speicher schreibt?
- 15.16. Wurde die Anwendung entwickelt um empfindliche Informationen zu verschlüsseln, die es einem anderen System übersendet?
- 15.17. Wurde die Anwendung entwickelt um empfindliche Informationen zu verschlüsseln, die es zu Cookies schreibt?
- 15.18. Ist die Anwendung unter Entwicklung, dafür entworfen worden, übermäßig voraussagbare Beglaubigung und Verschlüsselungscodes zu verhindern?
- 15.19. Ist die Anwendung unter Entwicklung, dafür entworfen worden, das Konzept von wenigsten Vorzug zu verwenden, wenn Instruktionen durchgeführt werden?
- 15.20. Wann immer möglich, ist die Bedeutung von Codebestandteilen maskiert oder verfinstert in den Anwendungen unter Entwicklung die entworfen wurden um kritische Operationen auszuführen?
- 15.21. Sind kritische Anwendungen unter Entwicklung, die entworfen wurden um Subbestandteile wie dynamische Verbindungsbibliotheken zu beglaubigen, bevor die verwendet werden? *

Die Sicherheitsprüfung der Neuen Software

- 15.22. Ist die Software, die die Vereinigung entworfen hat einer Codebewertung von einer Sicherheitseinstellung ausgesetzt worden, unabhängig davon ob es ausgegliedert oder innerbetrieblich erzeugt wurde, bevor die Endversion für die Aufstellung bereitgemacht wird? *
- 15.23 Sind irgendwelche Benutzerrechnungen die für Softwareprüfung verwendet wurden, systematisch entfernt, bevor die Software tatsächlich in Dienst gestellt wird?

- 15.24. Falls dort eingebettete Anmerkungen von Entwicklern auf dem Quellcode sind, die den Entwicklungsprozess überleben , werden diese Anmerkungen manuell entfernt, bevor das Programm eingesetzt wird?
- 15.25 Hat die Vereinigung Informationssicherheitsfachleute die Verwundbarkeitstests der Software ausführen, unabhängig davon ob es ausgegliedert oder innerbetrieblich erzeugt wurde?
- 15.26. Hat die Organisation Informationssicherheitsfachmänner die regelmäßige Verwundbarkeitsprüfungen gegen Anwendungen führen, nachdem sie eingesetzt werden?

Allee 16: Policen, um Sich mit Außenverkäufern zu befassen

Das Herstellen Passender Beziehungen mit Verkäufern

- 16.01. Hat die Vereinigung eine schriftliche Politik, die über die Schritte und Verfahren ausführlich berichtet, um sich mit Softwareverkäufern und Außenentwicklern zu befassen?
- 16.02. Sind zukünftige Verkäufer und Außenentwickler auf diejenigen beschränkt die nachgeprüft werden können , um Industriestandards für die Informationssicherheit zu entsprechen?
- 16.03. Sind Verkäufer oder Vertragspersonal erfordert Vorgespräche oder Ausbildungen in den Sicherheitspolicen der Kundenvereinigung zu haben?
- 16.04. Sind Verkäufer oder Vertragspersonal, vertraglich erforderlich an den Sicherheitspolicen der Kundenvereinigung anzuhaften?
- 16.05. Verlangen korporative Policen, das Verkäufer-Personal Geheimhaltungsvereinbarungen unterzeichnen?
- 16.06. Verlangen die Dienstabmachungen, das Verkäufer Werdegangkontrollen über ihr Personal führen, bevor sie der korporativen Rechnung zugeteilt werden?
- 16.07. Wenn die Anwendung von einem Drittenverkäufer geliefert wurde, kann der Verkäufer demonstrieren, das Vorsichtsmaßnahmen genommen wurden, um sicherzustellen, das die Anwendung nicht Hintertüren hat, die Drittenzugang erlauben?
- 16.08. Sind Softwareverkäufer erforderlich, zu bescheinigen, das ihr Code eine strikte und gründliche Sicherheitsprüfung durchgemacht hat, bevor es für die Aufstellung geliefert wird?
- 16.09. Sind Softwareverkäufer erforderlich, um Übertragungsurkunde-Vorbereitungen für die Bewahrung und Schutz des Quellcodes verwendet in den Anwendungen zu treffen, die gekauft werden oder lizenziert?

Das Handhaben Laufender Beziehungen mit Verkäufern

- 16.10. Gibt es vertraute Kanäle, um Aktualisierungen von jedem Softwareverkäufer zu erhalten?
- 16.11. Gibt es ein regelmäßiges Verfahren, um über das Internet oder telefonisch nachzuprüfen, dass physische Sendung vom Verkäufer eine authentische ist?
- 16.12. Versorgen Verkäufer physische Sendungen mit dem Verpacken und Etiketten die schwierig zu fälschen oder herumzubasteln sind?
- 16.13. Wenn Softwareaktualisierungen angewandt werden müssen, ist dort eine Garantie, daß diese Aktualisierungen in der relevanten Art der Softwareumgebung entsprechend geprüft wurden, bevor sie installiert werden?
- 16.14. Gibt es passende Beschränkungen und ein Verfallsdatum auf den Zugriffsrechten, daß die Verkäufer brauchen, um die Software und Aktualisierungen zu installieren?
- 16.15. Werden Schritte regelmäßig gemacht, um nachzuprüfen, das Zugriffsrechte für vorige Verkäufer und Auftragnehmer tatsächlich beseitigt wurden, sobald die nicht mehr notwendig waren?
- 16.16. Sind da Bestimmungen um die Leistung des Systems während des Aktualisierungsprozesses aufrechterhalten und das System zu seinem letzten bekannten guten Zustand wiederherzustellen, wenn eine Aktualisierung versagt?
- 16.17. Hat die Organisation Prozesse gegründet um inneren Informationszugang durch Außenverkäufer oder Auftragnehmer einzuschränken, zu kontrollieren, oder zu beobachten? *
- 16.18. Hat die Organisation Prozesse gegründet um Verkäufer, Auftragnehmer, und anderen ausgegliederten Personalzugang zu beenden, wenn es nicht mehr erforderlich ist?
- 16.19. Sind die Ankünfte Weggehen der Verkäufer geloggt und kontrolliert, entweder elektronisch oder physisch?
- 16.20. Gibt es Verfahren, um nachzuprüfen, das Kopien der Eigentumsinformationen zerstört wurden, nachdem die Verkäufer die geschlossene Software lieferten?
- 16.21. Sind die Handlungen von vorigen Verkäufern oder Auftragnehmern die kritische Informationen behandelten oder kritische Systeme kontrollierten für die Nichteinhaltung gegen Geheimhaltungsabkommen?