







IT SECURITY BUNDLE Angebot

Gebündelte Unterstützung mit der Swiss Infosec AG

Vorausschauende, präventive Massnahmen können existierenden Bedrohungen mit geringem Aufwand entgegenwirken. Der Stillstand des Unternehmens nach einem Ransomware-Angriff oder auch der Abfluss von sensiblen Geschäftsinformationen – beides sind unangenehme und oft auch kostspielige Umstände, welche sich vermeiden lassen.

Die Swiss Infosec AG bietet ein IT Security Bundle an, bestehend aus 4 Modulen:

Verwundbarkeits-analyse	Hardening Check	E-Mail Phishing	Webapplikation Penetration Test Light
			

Bei der Durchführung von mehr als einem Modul innerhalb von einem Jahr, ab Bestellung des ersten Moduls, erhalten Sie einen **Rabatt auf den Gesamtpreis der gebuchten Module:**

Bestellte Module	Rabatt	Konditionen
2	10%	Reduktion von 10% auf den Gesamtpreis der gebuchten Module.
3	15%	Reduktion von 15% auf den Gesamtpreis der gebuchten Module.
4	20%	Reduktion von 20% auf den Gesamtpreis der gebuchten Module.

Kontaktieren Sie uns jetzt für ein unverbindliches Angebot. Natürlich 100% vertraulich, kostenfrei und unverbindlich!



Die Verbindung von Spezialisten aus Recht (Datenschutz, IT-Recht), Informationssicherheit und Technik (IT-Sicherheit, Cybersecurity) macht uns zu Ihrem Partner für überzeugende Sicherheitslösungen bezüglich technischen und organisatorischen Massnahmen.

Unsere Spezialisten beantworten gerne Ihre Fragen rund um das Thema IT Security. Reto Steinmann, Head of Consulting, steht Ihnen gerne persönlich zur Verfügung:
+41 41 984 12 12, reto.steinmann@infosec.ch, www.infosec.ch/it-sicherheit



Verwundbarkeitsanalyse

Den Überblick über die Verwundbarkeit der eigenen Systemlandschaft zu behalten, stellt für IT-Betriebsverantwortliche eine Herausforderung dar. Mit einer Verwundbarkeitsanalyse unterstützen wir diesen Prozess und überprüfen Ihre Systemlandschaft auf ungeschützte Schnittstellen, unsichere Dienstprogramme, fehlende essenzielle Sicherheitseinstellungen und -updates und unsichere Verschlüsselung. Dabei kümmert sich ein Spezialist der Swiss Infosec AG darum, dass Ihr Unternehmen unkompliziert und schnell eine Übersicht existierender Schwachstellen innerhalb der Systemlandschaft erhält. Zudem wird die Vollständigkeit des System- und Anwendungsinventars geprüft werden. Nach der Beurteilung der Schwachstellen und den dazu empfohlenen Schutzmassnahmen erhalten Sie einen kumulierten und übersichtlichen Abschlussbericht über den Zustand Ihrer Systeme. Ein Sicherheitsspezialist der Swiss Infosec AG erläutert Ihnen im Rahmen einer Abschlussbesprechung die Befunde im Detail und unterstützt Sie bei der Definition von angemessenen und kosteneffizienten Optimierungsmassnahmen.



Hardening Check

Sollte es einem Angreifer einmal gelingen, ins Netzwerk Ihrer Organisation zu gelangen, wird er versuchen, sich auf andere Systeme auszubreiten. Diese laterale Ausbreitung gelingt oftmals, da Betriebssysteme zur Aufrechterhaltung der Kompatibilität mit älteren Systemen standardmässig veraltete Technologien zulassen. Solche (Fehl-)Konfigurationen können durch den Angreifer ohne Weiteres missbraucht werden, um weitere Systeme zu kompromittieren. Gerne helfen wir Ihnen dabei, sich einen Überblick über die sicherheitsrelevanten Einstellungen und existierendes Optimierungspotenzial für die sichere Konfiguration Ihrer Systeme zu schaffen. Stichprobenweise wird von einzelnen repräsentativen Systemen die bestehende Konfiguration auf mögliche Sicherheitsrisiken geprüft. Die Ergebnisse werden zusammen mit priorisierten Handlungsempfehlungen in einem kumulierten Bericht dokumentiert. Zu jedem Sicherheitsrisiko wird Ihnen aufgezeigt, welche Systemeinstellungen Sie vornehmen sollten. So oder so, auf die richtige «Einstellung» kommts an – wir helfen Ihnen gerne in einem abschliessenden persönlichen Gespräch dabei, Ihre Systeme resilienter zu betreiben!



E-Mail Phishing

Die grösste Chance ist der Mensch – jedoch können Menschen Fehler unterlaufen. Sei es aus Unwissenheit, Unachtsamkeit, fehlender Ausbildung oder man ist einfach einer Verlockung zum Opfer gefallen: technische Sicherheitsmassnahmen greifen nur so weit, wie der Mensch es durch sein Verhalten zulässt. Informationen über ein Unternehmen und seine Mitarbeitenden sind oft einfach öffentlich zu finden und werden zur Ausnutzung der «Schwachstelle Mensch» in einer Phishing E-Mail verwendet. Die Angreifenden nutzen hierbei soziale Faktoren aus, um dabei einen Menschen zu überzeugen, ein Dokument zu öffnen, einen Link zu betätigen und schlimmstenfalls das eigene Kennwort auf einer gefälschten Internetseite zu hinterlegen. Mit unseren individuell auf das Unternehmen abgestimmten Phishing-Kampagnen nutzen wir einen simulierten Phishing-Angriff zur Sensibilisierung Ihrer Mitarbeitenden. Diese Kampagnen können wie übliche Massen-E-Mails an ein ganzes Unternehmen oder individuell an spezifische Schlüsselpositionen gesandt werden. Unsere Sicherheitsspezialisten planen mit Ihnen die Kampagne, führen diese in einem definierten Zeitraum aus und analysieren gemeinsam mit Ihnen die Resultate. Wie sagt man so schön, Vorsorge ist Fürsorge, vor Allem für das Sicherheitsbewusstsein Ihrer Mitarbeitenden.



Webapplikations-Penetration Test Light

Webapplikationen mögen für nicht-technische Betrachter wenig komplex erscheinen, dahinter steckt jedoch oftmals ein komplexer Aufbau aus verschiedenen Komponenten, die zusammenarbeiten müssen, um dem Betrachter alle Funktionen anbieten zu können. Sei es ein Webshop, in dem ein Unternehmen seine Produkte zum Verkauf anbietet oder eine rein informative Website mit Kontaktformular – die Website kann für Unternehmen und Betrachter gleichermaßen zweckentfremdet werden. Angreifende verwenden dabei beispielsweise Eingabefelder, um an die Informationen von Kunden- und Administratorenkonten zu gelangen. Auch sind die im Hintergrund befindlichen Datenbanken, welche bspw. die Warenkörbe von Kunden beinhalten, bei ungenügendem Schutz ein Einfallstor für Manipulation der Daten oder weiterführender Schadsoftware. Sicherheitsspezialisten der Swiss Infosec AG überprüfen Ihre Webapplikation auf existierende Schwachstellen. Teils automatisiert und teils manuell werden Codefragmente der Website untersucht und angegriffen, ohne dabei Schaden zu verursachen. Die gefundenen Schwachstellen werden Ihnen in einem Bericht zusammengefasst und verständlich dargelegt und mit priorisierten Handlungsempfehlungen versehen.