Sicherheitsforum
Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

Sicherheitspreis Baden-Württemberg

Preisträger 2007–2019

Grußwort

Wirtschaftsspionage ist ein hoch aktuelles Thema – kaum eine Woche vergeht ohne spektakuläre Fälle, kaum eine Branche ist davor gefeit. Etwa jedes dritte Unternehmen in Deutschland ist von Wirtschaftsspionage betroffen. Mit dem erfolgreichen Einsatz ihres Know-how sichern die Unternehmen in Baden-Württemberg ihre Wettbewerbs- und Standortvorteile. Umso wichtiger ist es, dieses Know-how vor unberechtigten Zugriffen Dritter zu schützen. Dies gilt nicht nur für große Unternehmen, sondern auch für mittelständische Unternehmen, die immer häufiger von Spionageangriffen betroffen sind.

Mit dem „Sicherheitsforum – Die Wirtschaft schützt ihr Wissen" wurde 1999 ein unabhängiges und politisch nicht gebundenes Gremium aus Firmen, Forschungseinrichtungen, Verbänden, Kammern und Behörden des Landes Baden-Württemberg gegründet. Es hat sich zur Aufgabe gemacht, die heimische Wirtschaft und Forschung beim Schutz ihres Wissens und ihrer Innovationen zu unterstützen. Gerade vor dem Hintergrund einer hohen Dichte innovativer Firmen und wissenschaftlicher Einrichtungen in Baden-Württemberg und der Gefahren von Wirtschafts- und Konkurrenzspionage ist dies eine wichtige Aufgabe.

In diesem Jahr vergibt das Sicherheitsforum zum siebten Mal den Sicherheitspreis. Seit 2007 werden damit herausragende Projekte der betrieblichen Sicherheit ausgezeichnet, die dem Schutz von Know-how dienen. Die Vergabe des Sicherheitspreises soll dazu beitragen, das Bewusstsein für die Sicherheit zu erhöhen und Unternehmen sowie Organisationen zu sensibilisieren. Auch mit der diesjährigen Preisvergabe wird das hohe Innovationspotenzial baden-württembergischer Unternehmen dokumentiert.

Wir danken allen Unternehmen für ihre Teilnahme am Sicherheitspreis. Damit stellen sie ihr hohes Interesse für den Schutz von Know-how am Wirtschafts-

standort Baden-Württemberg und ihr innovatives Handeln unter Beweis. Unser Glückwunsch gilt den ausgezeichneten Unternehmen.

Thomas Strobl
Stellvertretender Ministerpräsident
und Minister für Inneres, Digitalisierung und
Migration des Landes Baden-Württemberg

Dr. Nicole Hoffmeister-Kraut
Ministerin für Wirtschaft, Arbeit und Wohnungsbau
des Landes Baden-Württemberg

Inhalt

Der Sicherheitspreis Baden-Württemberg

Das Sicherheitsforum Baden-Württemberg vergibt 2019 zum siebten Mal den Sicherheitspreis für herausragende Projekte der betrieblichen Sicherheit mit der Zielsetzung Know-how-Schutz. Als besonders auszeichnungswürdig werden mustergültige Projekte zur praxisgerechten Konzeption, Realisierung und Kontrolle unternehmensinterner Sicherheitsmaßnahmen betrachtet. Dabei kann es sich sowohl um die Optimierung bereits vorhandener Strukturen als auch um die Implementierung völlig neuer Mechanismen handeln. Eingereicht werden können Projekte des personellen, technischen, organisatorischen oder rechtlichen Informationsschutzes. Alle ausgezeichneten Projekte leisten einen Beitrag zum Innovationspotenzial des Landes.

Die Vergabe des Sicherheitspreises soll nicht nur in hohem Maße zur Sensibilisierung und Steigerung des Sicherheitsbewusstseins in den Unternehmen und Organisationen generell beitragen, sondern auch das Innovationspotenzial in Baden-Württemberg auf dem Sektor Sicherheit dokumentieren und fördern. Die Möglichkeit zur Präsentation von ausgezeichneten Best-Practice-Projekten, verbunden mit der Diskussion von Meinungs- und Technologieführern auf dem Gebiet der Sicherheit, eröffnet Chancen, Entwicklungen aus diesem Bereich zu beeinflussen und auch andere Institutionen für die Gefahr des ungewollten Know-how-Abflusses zu sensibilisieren. Somit könnte diese Möglichkeit zur Initialzündung für eine umfassende, auch volkswirtschaftliche Aspekte berücksichtigende Auseinandersetzung mit dem Thema Know-how-Schutz werden.


Sicherheitspreis
Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

Preisträger 2007–2019

1. Preis 2019: Sicherheitstechnik Sancak e.K.

Projekt Automatisierter Zutritt: Das Smartphone als komfortable und sichere Zutrittslösung für Besucher/Mitarbeiter

ELOCK2 ist ein Technologieunternehmen in dritter Generation – stetig auf der Suche nach neuen Lösungen. Für Investoren und Betreiber im Bereich der Gebäudesicherung wird in den nächsten Jahren Kernthema sein, wie sich Smartphones als Besucher-/Mitarbeiterschlüssel einsetzen lassen. Projektziel war es, die Umsetzung der automatisierten Zutrittskontrolle in die Sicherheitsschlösser mit einzigartiger Mechanik zu integrieren und zugleich bestehende Normen und Anforderungen an Fluchtweg, Brandschutz und Einbruchhemmung beizubehalten.

Das Zutrittsmanagement erfolgt flexibel durch die Systemsoftware, sichere Transponder, Smartphones via Web-Oberflächen oder die ELOCK2-Apps. Die Soft- und Hardware-Schnittstellen erlauben die Verbindung zu Fremdsystemen und kundenspezifischen Anpassungen. Das Entwicklungsteam von ELOCK2 setzte das Projekt Ende 2017 um. Verschiedene Möglichkeiten wurden für Besucher/Mitarbeiter mit der ELOCK2-App aufgezeigt: So vereinfacht die ELOCK2-Funktion „Push to Open“ den Berechtigungsprozess und verlängert die Lebensdauer der Komponenten. Die Besonderheit des Konzeptes liegt darin, dass eine nahtlose Integration in bestehende Zutrittssysteme und Konzernausweise möglich ist. Außerdem kann das Projekt auf andere Anwendungen übertragen werden: Im Bereich der Produktion kann beispielsweise sichergestellt werden, dass die Maschinen nur aktiv sind, solange sich das zugehörige Personal mit dem Smartphone neben der Maschine befindet. Ein weiteres wichtiges Feature der ELOCK2-App ist seine Over-the-Air-Fähigkeit. Dadurch lässt sich das Smartphone nach Bedarf von einer zentralen Stelle (Mobile Device Management) über eine Luftschnittstelle konfigurieren. So können einzelnen Token über das Mobilfunknetz – sicher, spontan und ortsunabhängig – neue Berechtigungen zugewiesen oder entzogen werden. Damit kann das Projekt selbst komplexen Sicherheitsanforderungen gerecht werden.

Sicherheitstechnik Sancak e.K. | Esslingen
https://sancak.info/


ELOCK2
9:41
Tuesday, September 12
ELOCK2
Auto unlocked Office 42
now


SCHWEICKERT
VON STROM BIS IT

2. Preis 2019: Schweickert Netzwerktechnik GmbH

Projekt Webanwendung für ein Internet Security Audit

Vor über 50 Jahren begann die Erfolgsgeschichte von Schweickert. Seitdem hat sich das inhabergeführte Unternehmen an zehn Standorten zu einem weltweit tätigen Unternehmen mit über 450 Mitarbeitern entwickelt. Schweickert bietet mit einem kompetenten Team an Technikern und Ingenieuren maßgeschneiderte und komplexe IT-Lösungen sowie individuelle, wirtschaftliche Komplettlösungen in den Bereichen Gebäude-, Elektro- und Sicherheitstechnik an.

Ziel von Schweickert war es, eine standardisierte und auswertbare Ist-Aufnahme der Informationssicherheit im eigenen Unternehmen durchzuführen. Hierzu wurden eine Checkliste und weitere Vorlagen genutzt, die auf einem Fragenkatalog des Verbandes der deutschen Automobilindustrie (VDA) basieren, welcher die organisatorische Sicherheit prüft. Dieser wurde wiederum durch eine Sammlung sicherheitstechnischer Fragen ergänzt.

Das Erheben der Daten in dieser Form ist ein „Papierkrieg“ in Verbindung mit Excel-Listen, einem Maßnahmenplan in Word sowie einer Management-Präsentation in PowerPoint. Bei den Vorbereitungen zum Audit war Jonas Bohn, DH-Student bei Schweickert, beteiligt. Er hatte im Nachgang die Idee, den kompletten Check als Webanwendung im Rahmen seiner Bachelorarbeit zu entwickeln.

Mit der von Jonas Bohn entwickelten Applikation ist es nun möglich, in einer einzigen Anwendung zu arbeiten, den Reifegrad der Informationssicherheit nachzuverfolgen und dies ohne redundante Informationen in unterschiedlichen Dateien. Mithilfe der Software-Applikation wurde die Komplexität des Audits nachhaltig verringert und ein Hilfesystem entwickelt, das es dem Auditor ermöglicht, komplette Prozesse flexibel und standardisiert zu analysieren.

Schweickert Netzwerktechnik GmbH | Walldorf
www.schweickert.de

2. Preis 2019: Robert Bosch GmbH

Projekt One-Security-Awareness-Tag am Bosch Standort Karlsruhe: ganzheitlich und praxisnah

Der Bosch-Geschäftsbereich Automotive Aftermarket begreift Sicherheit ganzheitlich: Verschiedene Blickwinkel müssen berücksichtigt werden, um Risiken zu erkennen, zu identifizieren, angemessen zu behandeln und damit einen aktiven Beitrag zur Geschäftsstrategie zu leisten.

Im Jahr 2018 stand diesbezüglich die Steigerung der themenübergreifenden Awareness im Fokus – eingebettet in eine dreijährige, gemeinsam mit Kommunikationsexperten ausgearbeitete Kampagne. Da gerade Cyber- und physische Sicherheit zunehmend miteinander verwoben sind und gleichzeitig Schnittstellen beispielsweise zu Compliance, zum Personalwesen oder auch zum Liegenschaftsmanagement bestehen, wurde in Karlsruhe im zweiten Halbjahr 2018 eine abteilungsübergreifend abgestimmte Kampagne durchgeführt. Zielsetzung war die Erhöhung des Sicherheitsbewusstseins im Allgemeinen, jedoch insbesondere eine konkrete jeweilige Verhaltensänderung im täglichen Arbeitsleben, zum Beispiel mit Blick auf die Themen Wirtschaftsspionage, Social Engineering, Datenschutz, Compliance, Reisesicherheit oder auch Logistik. Mit simulierten Phishing-E-Mails, Kurzfilmen und anderen Medien wurden die Mitarbeiter über mehrere Monate hinweg zielgerichtet sensibilisiert, reale Gefahren aufgezeigt und Handlungsmöglichkeiten vorgestellt.

Ein Höhepunkt am Standort war der One-Security-Awareness-Tag mit spannenden internen und externen Vorträgen sowie vielfältigen Möglichkeiten zur Interaktion (Marktstände, Fotobox, USB-Stick-Überprüfung, offene Diskussionrunden etc.). Vergleichbare Veranstaltungen wurden – jeweils standortbezogen fokussiert – an allen drei Hauptstandorten des Geschäftsbereichs durchgeführt und werden zukünftig wiederholt stattfinden.

Robert Bosch GmbH | Karlsruhe
www.bosch.com


BOSCH


Sicherheitsforum
Baden-Württemberg
1. Preis 2017

1. Preis 2017: SICK AG

Projekt Einführung eines konzernweiten Informationssicherheits-programms

Die SICK AG hat bereits im Jahr 2009 begonnen, die Anforderungen des unternehmenseigenen Verhaltenskodex „Der umsichtige Umgang mit vertraulichen Informationen und internem Wissen schützt die SICK" in Form eines Informationssicherheitsprogramms umzusetzen. Beginnend mit dem Stammhaus in Waldkirch werden die Vorgaben der ISO 27001 nach und nach im ganzen Konzern eingeführt und die zentralen IT-Services schrittweise mittels eines ISMS bis zur Zertifizierung in 2017 herangeführt.

Realisiert wurde dies im technischen Bereich durch regelmäßige Penetrationstests und interne ISO 27001-Audits, die zu einer Verbesserung der IT-Sicherheitstechnologien samt Verschlüsselungs- und Authentifizierungssystemen geführt haben. Außerdem wurden Mindestsicherheitsstandards (IS-Policies) definiert, die ein Musterregelwerk für Informationssicherheit und Datenschutz darstellen, das mit dem Landesdatenschutz Baden-Württemberg sowie dem Cyber-Sicherheits-Check des Bundesamts für Sicherheit in der Informationstechnik (BSI) abgestimmt ist.

Im personellen und organisatorischen Bereich setzt die SICK AG auf Sensibilisierungskampagnen, regelmäßige Präsenztrainings und eLearnings. Damit wird das Sicherheitsbewusstsein der Mitarbeiter und deren Kenntnis über die IS-Policies auf einem hohen Niveau gehalten. Außerdem wurde ein konzernweites „Information Security Officer Experten Netzwerk" aufgebaut, bei dem speziell geschulte Mitarbeiter die Sicherheit und den Datenschutz ständig überwachen, auswerten und Sicherheitsgefährdungen an die Zentrale melden. Das Informationssicherheitsprogramm wurde parallel zum Datenschutzmanagementsystem aufgebaut und wirkt synergetisch im Bereich der technischen und organisatorischen Maßnahmen. Über die Mitwirkung des Unternehmens im Südwestmetall AK „Informationssicherheit" konnte auch erfolgreich ein Mehrwert für andere Mitgliedsfirmen in Baden-Württemberg realisiert werden.

SICK AG | Waldkirch
www.sick.com

2. Preis 2017: Herrenknecht AG

Projekt „Together we are securing our future“

Das Projekt der Herrenknecht AG ist nicht auf technische, sondern auf menschliche Maßnahmen ausgerichtet. Kernstück des Sicherheitskonzepts ist die Sensibilisierung aller Mitarbeiter in ihrem täglichen Umgang mit Unternehmens- und Personendaten, insbesondere sicherheitsrelevanten und sensiblen Informationen. Dabei wird auch externe Fachkompetenz, wie zum Beispiel die des Landesamtes für Verfassungsschutz, genutzt und eingebunden.

Durch praxisnahe diverse Awareness-Kampagnen und Trainings – sowohl national als auch international – wird eine entsprechende Sicherheitskultur in der Herrenknecht-Unternehmensgruppe gebildet und gefördert. So werden mit praxisnahen Beispielen, zielgerichteten Aktionen und dem Einsatz verschiedener Medien alle Mitarbeiter in den Bereichen Informationssicherheit, Technologieschutz und Cyber Crime geschult. Außerdem wurde eine fachübergreifende Zusammenarbeit von zentralen Abteilungen des Unternehmens in Sicherheitsfragen etabliert.

Durch die regelmäßigen Schulungsmaßnahmen werden die Themen nachhaltig vermittelt, und jeder fühlt sich als Teil des Ganzen. Sowohl Verhaltensänderungen als auch Sensibilisierung der Mitarbeiter sind erkennbar.

Herrenknecht AG | Schwanau
www.herrenknecht.com


Sicherheitspreis
Baden-Württemberg
Sicherheitsforum
Baden-Württemberg
Das Sicherheitsforum Baden-Württemberg
2. Preis 2017
Herrenknecht AG
Schwanau
„Together we are
securing our future"


Sicherheitspreis
Baden-Württemberg
Sicherheitsforum
Baden-Württemberg
2. Preis 2017

2. Preis 2017: IHK Rhein-Neckar

Projekt IHK-Arbeitskreis „Sicherheit in der Wirtschaft“ als Netzwerkdrehscheibe der Unternehmenssicherheit

Der Arbeitskreis „Sicherheit in der Wirtschaft“ der IHK Rhein-Neckar bietet seit Jahren eine Plattform für Erfahrungsaustausch, Information und Diskussion zwischen den Sicherheitsverantwortlichen der Mitgliedsunternehmen und Vertretern von Behörden, Fachfirmen und Sicherheitsorganisationen. In drei Veranstaltungen pro Jahr werden im Rahmen von Vorträgen, Workshops, Podiumsdiskussionen, Exkursionen und Präsentationen mit Themenschwerpunkten aus den Bereichen IT-Security, Spionage, Brand- und Explosionsschutz, Arbeits- und Umweltschutz sowie Unternehmenssicherheit/Werkschutz behandelt. Derzeit profitieren ca. 170 Sicherheitsverantwortliche aus den Mitgliedsfirmen der IHK Rhein-Neckar und der IHK Pfalz von diesem kostenlosen Angebot. Umgekehrt legen auch die in der Region beheimateten Sicherheitsorganisationen, wie zum Beispiel Landesämter für Verfassungsschutz, Feuerwehren, Rettungsdienste und Polizeidirektionen, großen Wert darauf, mit diesem Arbeitskreis verbunden zu sein und vom direkten Kontakt zu den Unternehmen zu profitieren. Diese Sicherheitspartnerschaft ist somit nicht nur einseitig angelegt von Unternehmen zu den Sicherheitsbehörden, sondern auch umgekehrt. Für Großunternehmen selbstverständlich, ist die betriebliche Sicherheit für kleinere Firmen oft nur ein Randthema. Der Arbeitskreis bietet und fördert bewusst den formellen Austausch im Rahmen der Treffen sowie den informellen Austausch auf persönlicher Ebene unterjährig, sodass der Arbeitskreis als „Katalysator“ dazu beiträgt, Informationen aus dem Kreis der Sicherheitsverantwortlichen in Unternehmen laufend gegenseitig auszutauschen und aktuellen Themen nachzugehen. Das Netzwerk ist dabei keineswegs als passiver Informationsverteiler angelegt, vielmehr befruchtet es sich immer wieder aus sich selbst heraus mit neuen Inhalten und Themen. Die IHK Rhein-Neckar hat es zusammen mit der IHK Pfalz geschafft, mit dieser Initiative das Bewusstsein für Sicherheitsthemen insbesondere bei kleinen und mittelständischen Unternehmen der Region zu stärken und zu sensibilisieren.

Industrie- und Handelskammer Rhein-Neckar Mannheim | www.rhein-neckar.ihk24.de

1. Preis 2015: J. Schmalz GmbH

Projekt IT-Notfallmanagement „ISMS-Notfall“

„Risiken kennen, Herausforderungen annehmen, Lösungen gestalten“, lautet das Motto der J. Schmalz GmbH, wenn es um die sichere Vernetzung von IT-Systemen im Unternehmen geht. Dabei steht bei jeder Lösung der Mensch im Zentrum der Technik.

Wie jedes andere Unternehmen verfügt auch die J. Schmalz GmbH über eine Vielzahl an Unternehmensinformationen, die den Wert des Unternehmens repräsentieren und daher besonderen Schutz- und Zugriffsmethoden unterliegen. Sicherheitsvorfälle der Vergangenheit haben gezeigt, dass die bereits etablierten Methoden noch optimiert werden können. Mit der Einführung eines Sicherheitsmanagementsystems (ISMS) wollte sich das mittelständische Unternehmen vor den unerlaubten Zugriffen schützen. Eine wichtige Rolle spielte dabei die Einführung und Umsetzung eines IT-Notfallmanagementsystems auf Grundlage eines bereits vorhandenen Ticketing Systems mit dem Ziel, den IT-Notfallprozess in das Tagesgeschäft der IT-Abteilung zu integrieren.

Als erstes wurde ein auf theoretischen Erkenntnissen basierender Projektplan erstellt, der im nächsten Schritt auf die Gegebenheiten des Unternehmens angepasst wurde. Einer der wichtigsten Realisierungsschritte des Projektes bestand darin, das Bewusstsein für die „Sensibilisierung“ im gesamten Unternehmen unter anderem mithilfe einer Awareness-Kampagne zu schaffen. Des Weiteren wurde ein Notfallmanagementprozess initialisiert, umgesetzt und in die Linienfunktion übergeben. Dass die Projektumsetzung erfolgreich war, zeigt das durch die DEKRA im September 2014 durchgeführte Überwachungsaudit ISO 9001:2008, in dem das neue IT-Notfallmanagementsystem positiv hervorgehoben wurde.

J. Schmalz GmbH | Glatten
www.schmalz.com


Sicherheitsforum
Baden-Württemberg
Die Wirtschaft schützt ihr Wissen
Das Sicherheitsforum Baden-Württemberg


Notfall
Sicherheitsforum
Baden-Württemberg
2. Preis 2015
Ernst Umformtechnik GmbH
Oberkirch-Zusenhofen
Sensibilisierung als Basis
zur Globalisierung

2. Preis 2015:
Ernst Umformtechnik GmbH

Projekt Sensibilisierung als Basis zur Globalisierung

Die Ernst Umformtechnik GmbH ist ein erfolgreicher mittelständischer Automobilzulieferer, der im Zuge seiner Internationalisierung (Niederlassungen in Frankreich, USA und China) der IT-Sicherheit immer schon besonderes Augenmerk geschenkt hat. Dazu zählen die äußerst restriktive Verwaltung von Schnittstellen jeglicher Art, die Einführung einer zweistufigen Firewall-Absicherung, die Erstellung einer stringenten Passwortrichtlinie sowie die konsequente Beschränkung auf firmenspezifische Informationstechnik.

Im Rahmen des aktuellen Projektes wurde die IT-Infrastruktur komplett neu aufgesetzt. Es wurde an jedem Standort eine autarke IT eingerichtet, die ihrerseits nur vom deutschen Stammsitz in Oberkirch-Zusenhofen aus angesteuert werden kann, die umgekehrte Einwahl aus dem Ausland dagegen nicht ermöglicht. Die Beschaffung, Installation und Inbetriebnahme sämtlicher Systeme, inklusive mobiler Endgeräte, erfolgte in Deutschland oder zumindest von Deutschland aus.

Die dargestellten IT-Sicherheitsmaßnahmen wurden begleitet durch Sensibilisierungsvorträge zum Thema Wirtschaftsspionage/Wirtschaftsschutz für die Mitarbeiter verschiedener Hierarchieebenen des Unternehmens – von der Geschäftsleitung über das Management bis hin zu sämtlichen Mitarbeitern, die in Kontakt mit den Niederlassungen im Ausland stehen. Solche Schulungen sollen auch in Zukunft ein wichtiges Element des unternehmensinternen Sicherheitskonzepts bleiben. Das Bewusstsein der Belegschaft für Spionagerisiken konnte ferner durch die organisatorischen und IT-technischen Aktivitäten des Unternehmens nachhaltig gesteigert werden. Als Mitglied des „IT-Strategieforums Baden“ (ca. 80 IT-Leiter vorwiegend kleinerer und mittelständischer Firmen) stellt die Firma Ernst ihre Maßnahmen und Erfahrungen auch den anderen Mitgliedsfirmen zur Verfügung.

Ernst Umformtechnik GmbH
Oberkirch-Zusenhofen | www.ernst.de

1. Preis 2013: Maschinenfabrik Gustav EIRICH GmbH & Co KG

Projekt Mitarbeitersensibilisierung bei Eirich – Sicherheit ohne Technik

Laut einer Studie des Sicherheitsforums Baden-Württemberg kommen 70% der Täter bei ungewolltem Know-how-Abfluss aus dem eigenen Unternehmen. Neben den technischen Schutzmaßnahmen gehört deshalb die Sensibilisierung aller Mitarbeiter für Informationsschutz zu den wichtigsten Aufgaben der Informationssicherheit. Ziel der Awareness-Kampagne „Sicherheit ohne Technik" bei der Maschinenfabrik Gustav Eirich war es, das Sicherheitsbewusstsein der Mitarbeiter im Umgang mit Informationen zu steigern. Im Kern geht es darum, Gefahren rechtzeitig zu erkennen, Schaden durch Informationsabwanderung zu vermeiden und somit Know-how zu schützen, aber auch einen Mehrwert für das private Umfeld zuhause zu schaffen. Für die Umsetzung des Projektes war ein fachübergreifendes Team von Mitarbeitern verantwortlich. Zunächst wurden in einer anonymisierten Umfrage unter den Mitarbeitern Bedarfe in der Informationssicherheit am Arbeitsplatz abgefragt. Risiken und bekannte Vorfälle wurden gesammelt, der Ist-Wissensstand im Umgang mit Informationen festgestellt und Schulungsinhalte abgeleitet. In umfangreichen Schulungen wurden vom Geschäftsführer bis zur Hilfskraft ausnahmslos alle über 700 Mitarbeiter in einem dreistufigen Konzept zur Informationssicherheit geschult.

Wichtiger Bestandteil der Schulungen waren auch einige Give-Aways wie zum Beispiel eine Brotdose mit dem Slogan „Mit Sicherheit mehr drin", die den Charakter der Kampagne widerspiegelt und gleichzeitig durch den täglichen Gebrauch der Nachhaltigkeit dient.

Die Evaluierung zeigt, dass die Ziele des Projektes erreicht wurden. Eirich sieht einen Mehrwert in Form einer Signalwirkung gegenüber Kunden und Lieferanten. Bei den Planungen berücksichtigt war ferner die Ausweitung der Kampagne auf alle Schwestergesellschaften der Gruppe weltweit.

Maschinenfabrik Gustav EIRICH GmbH & Co KG
Hardheim | www.eirich.com


1. Preis 2013
Sicherheitspreis
Baden-Württemberg

2. Preis 2013: SAP AG

Projekt SAP Security Awareness Framework

Mit der Einführung des Security Awareness Framework hat SAP ein umfassendes Regelwerk an wiederkehrenden Sicherheitspflichttrainings, rollen- und prozessabhängigen Sicherheitstrainings und geschäftsbereichsspezifischen Trainings eingeführt, die die Sicherheit von SAP gewährleisten sollen. Das Projekt setzt sich zusammen aus Sensibilisierungskampagnen, Trainings/eLearnings zum Informationsschutz und einer nachhaltigen Strategie, um das Sicherheitsbewusstsein konstant hochzuhalten.

Das Ziel des Security Awareness Framework ist es, die SAP Mitarbeiter über Bedrohungen und Risiken zu unterrichten und folgende Maßnahmen innerhalb SAP sicherzustellen:

- Schutz von SAP-Mitarbeitern, Vermögenswerten, Informationen, geistigem Eigentum und Systemen,
- Ruf als sicheren und vertrauenswürdigen Partner behalten,
- Erfüllung gesetzlicher und vertraglicher Vorgaben,
- Erfüllung von Audits, Zertifizierungen und Compliance.

Die Besonderheit des Security Awareness Framework von SAP liegt darin, dass es langfristig angelegt ist und auf die unterschiedlichen Bedürfnisse der Mitarbeiter und deren Rollen eingeht. Erstmalig wurde bei diesem Pflichttraining für alle Mitarbeiter ein Assessment integriert, mit dem das Verständnis der vermittelten Inhalte überprüft wird. Das Training ist interaktiv, dauert rund eine Stunde und wird von nun an alle zwei Jahre wiederholt. Die eLearnings sind in das SAP Learning Portal integriert, über das die Mitarbeiter Zugriff auf die Trainings haben.

Als Leitmotiv für die 2012 eingeführte Sicherheitskampagne wählte SAP die „Human Firewall“, in die sich jeder SAP-Mitarbeiter „einreihen“ muss. Denn auch wenn sich Unternehmen technisch sehr gut gegen Angriffe von außen absichern können, kann die „menschliche Lücke“ in der Human Firewall mindestens genauso große Schäden anrichten.

SAP AG | Walldorf
www.sap.com

2. Preis 2013: COMback GmbH

Projekt Zertifizierung aller Geschäftsprozesse nach ISO 27001 auf Basis BSI Grundschutz

Die COMback GmbH hat eine unternehmensweite ganzheitliche Sicherheitsstrategie umgesetzt mit dem Ziel einer dauerhaft aufrecht zu erhaltenden Zertifizierung aller Geschäftsprozesse des Unternehmens nach ISO 27001 auf Basis BSI Grundschutz für hohen und sehr hohen Schutzbedarf. Der herausragende Sicherheitsstandard von COMback umfasst insbesondere auch die Realisierung eines ganzheitlichen Informationsschutzkonzepts mit ausgeklügelten personellen, materiellen, organisatorischen und IT-Sicherheitsmaßnahmen.

COMback wurde 1995 als Projekt mit Solidarcharakter von einem deutschen Systemhaus unter Mitträgerschaft einiger Partner und Kunden, darunter auch die Finanzverwaltung des Landes Baden-Württemberg, ins Leben gerufen. Zweck war, ein technisch tragfähiges und wirtschaftlich vertretbares Disaster Recovery-Zentrum zur Absicherung der IT-Infrastrukturen aller Beteiligten nach einem sogenannten Katastrophen-Fall zu schaffen. Im Jahr 2000 wurde das Projekt in ein eigenständiges Unternehmen überführt. 2007 hat die Unternehmensleitung beschlossen, die „Gelebte Sicherheit" durch eine entsprechende Zertifizierung zu dokumentieren. Dabei wurde unter Mitwirkung aller Mitarbeiter beschlossen, eine Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz für hohen und höchsten Schutzbedarf anzustreben und zwar für ausnahmslos alle Prozesse des Unternehmens. Das Ziel wurde 2009 erreicht, wird regelmäßig in Reauditierungen bestätigt und anhand von Key Performance Indicators gemessen. Im Sommer 2012 erfolgte nach drei Jahren die erfolgreiche Rezertifizierung. Der Zwang zu laufender Überprüfung wirkte sich bereits nach kurzer Zeit positiv auf den Mittel- beziehungsweise Arbeitseinsatz aus und kann daher als erkennbar kostenreduzierend bezeichnet werden. Kleine und mittelständische Unternehmen können auf das Dienstleistungsangebot von COMback, Fremddaten unter Hochsicherheitsbedingungen vorzuhalten, zurückgreifen.

COMback GmbH | Oberreichenbach
www.comback.de


Sicherheitsforum
Baden-Württemberg
2. Preis 2013


Sicherheitsforum
Baden-Württemberg
1. Preis
2011

1. Preis 2011: WIBU-Systems AG

Projekt Pro-Protect: Produktpiraterie verhindern mit Softwareschutz

Ziel des Projektes Pro-Protect war es, im Desktop-PC-Bereich existierende Softwareschutzlösungen auf den Bereich der Produktion zu übertragen und an die spezifischen Anforderungen und Bedürfnisse im Maschinen- und Anlagenbau anzupassen, um so einen durchgängigen Schutz vor den Gefahren der Produktpiraterie zu erreichen. Dabei sollten sowohl der Nachbau von Maschinen und Komponenten verhindert werden, die mit komplexen Software-Funktionen ausgestattet sind, als auch Methoden und Verfahren abgewehrt werden, die auf das nicht autorisierte Kopieren und Nutzen von aufwändigen Maschinensteuerungsprogrammen zur Herstellung von geklonten Produkten abzielen.

Die erreichten Ergebnisse können als substanzielle Neuerung eingestuft werden. Zu Projektbeginn gab es keine kostengünstigen standardisierten Lösungen, die einfach zu integrieren sind, nachrüstbar sind und über einen hohen Schutzgrad verfügten. Stattdessen wurden einzelne Lösungen von Herstellern selbst entwickelt, abseits von deren Kernkompetenz, was in viel Aufwand bei teilweise nur geringem Schutzgrad endete. Übergreifende Lösungen, die sowohl Maschinen, als auch Servicedokumente und Produktionsdaten schützen, gab es nicht.

WIBU-Systems AG | Karlsruhe
www.wibu.de

2. Preis 2011: Cytec Industries Inc.

Projekt Cybarry & Samantha Safe – der Expedition Security Podcast der Cytec

Bei „Cybarry & Samantha Safe“ handelt es sich um das laufende, seit 2010 durchgeführte Security Awareness-Maßnahmen-Paket der Cytec als Teil der seit 2009 weltweit an mehr als 60 Standorten gelaunchten internationalen Awareness-Gesamtkampagne „Expedition Security“ und auf Basis der wahrscheinlich ersten Security Awareness-Podcasts überhaupt.

Im Februar 2010 wurden von einem Team in Köln acht Folgen sowie ein Trailer in sechs Sprachen und damit insgesamt 54 Folgen des Security Awareness-Podcasts mit einer Gesamtlänge von knapp 400 Minuten produziert. Grundlage der Podcasts waren die bis dato publizierten Awareness-Comics mit Cybarry, der Leitfigur der Kampagne.

Die unterschiedlichen Folgen widmen sich jeweils einem anderen Informationsschutzthema und wurden ab April 2010 (Trailer) in einem monatlichem Rhythmus bis Dezember 2010 über das Cytec-Infosec-Intranet publiziert. Im Rahmen der Kampagne wurden die Podcasts darüber hinaus auch als sogenannte Kommunikationsbeschleuniger eingesetzt, beispielsweise innerhalb von „Lunch & Learn“-Sessions, denn Awareness wird vor allem über die unmittelbare Auseinandersetzung der Mitarbeiter mit dem Thema Sicherheit geschaffen.

Cytec Industries Inc. | Östringen


Monitoring | Speicherlösungen
Sicherheitsforum
Baden-Württemberg


Sicherheitsforum
Baden-Württemberg

2. Preis 2011: Festo AG & Co. KG

Projekt Effektiver und effizienter Know-how-Schutz für den Maschinen- und Anlagenbau

Im Rahmen des vom BMBF geförderten Forschungsprojektes ProOriginal entwickelte Festo zusammen mit Partnern aus Forschung und Industrie eine praxisnahe Lösung hinsichtlich eines erfolgreichen Know-how-Schutzes für den Maschinen- und Anlagenbau. Schlüssel ist ein innovatives Schutzkonzept, das aus den drei Maßnahmenbereichen „Recht", „Technik" und „Organisation" die passenden Schutzmaßnahmen miteinander vernetzt. Die konsequente Umsetzung der Forschungsergebnisse bei Festo beweist die Wirksamkeit dieser Strategie.

Nachahmung von Produkten und Umsatzeinbußen sind die eine Seite, Imageklau und Markenschädigung die andere. Gefahr erkannt, Gefahr gebannt: Mit der Entwicklung und Implementierung einer nachhaltigen und weitreichenden Schutzstrategie macht Festo einen bedeutenden Schritt im Kampf gegen Produktpiraterie und ihre Folgen.

Um das Ziel eines ganzheitlichen Schutzes von Know-how und Fachwissen zu erreichen und eine praxisorientierte Methodik zu entwickeln, ist für Festo die Zusammenarbeit mit Beteiligten entlang der gesamten Wertschöpfungskette unerlässlich. ProOriginal ist das daraus entstandene Verbundprojekt diverser Partner aus Industrie und Forschung, für das Festo im Jahr 2008 die Konsortialführerschaft übernahm.

Eng angelehnt an das von ProOriginal entwickelte „Darmstädter Modell" erfolgten sukzessive die einzelnen Realisierungsschritte des Projektes bei Festo. Nach intensiven Analysen der Ist-Situation, verbunden mit der Neuentwicklung von Konzepten zum Schutz der Ressource Wissen, begann im Jahr 2009 die operative Umsetzung im Konzern.

Festo AG & Co. KG | Esslingen
www.festo.com

1. Preis 2009: Wallenwein Facility Management GmbH

Projekt „i-safety“ Intelligentes Wächterkontrollsystem mit Elektronischem Wachbuch, in Verbindung mit integriertem Sicherheitsmanagement

Wie kaum ein anderer Dienstleistungsbereich ist der Wachdienst angehalten, sein Wirken in vielfacher Weise zu dokumentieren. Wachbucheinträge, Besucher- und Schlüssellisten, Listen für Reinigungskräfte, Poolfahrzeuge oder Dienstübergaben müssen erfasst und geführt werden.

Wallenwein hat dazu ein intelligentes internetbasiertes Wächterkontrollsystem (i-safety) mit Elektronischem Wachbuch und weiteren sicherheitsrelevanten Funktionen entwickelt. Durch die Nutzung des intelligenten Diensthandys „i-safety“ ist es möglich, eine Reihe von Sicherheits- und Qualitätssicherungsmaßnahmen während der Kontrollgänge effizient und sofort umzusetzen oder einzubinden, wie zum Beispiel die Erfassung von Wachmeldungen via Diensthandy einschließlich der Fotodokumentation in Echtzeit.

Das System ist technisch so vorbereitet und konzipiert, dass es auch sinnvoll in anderen Bereichen Anwendung finden wird, so zum Beispiel in Arbeitssicherheit und Arbeitsschutz, bei der mobilen Auftragsabwicklung und zur Datenerfassung bei Hausverwaltungen zur Steuerung und Koordination von Hausmeistern.

Wallenwein Facility Management GmbH
Stuttgart | www.fm24.info


chnik
ronik
Sicherheitsforum Baden-Württemberg
1. Preis 2009


Sicherheitsforum
Baden-Württemberg
2. Preis 2009

2. Preis 2009:
Edelstahl Rosswag GmbH

Projekt Neuordnung IT-Sicherheit und Datenschutz

Das Unternehmen beabsichtigte, die bisher an drei verschiedenen firmeninternen Standorten verteilte Serverstruktur im laufenden Betrieb in eine standardisierte und den Anforderungen höchster Sicherheit und Verfügbarkeit gerecht werdende Serverarchitektur zu überführen. Programmtechnisch veraltete Software war dabei in die neue Umgebung zu integrieren. Im Zuge dieser Umstellung wurden umfassende technische und organisatorische Maßnahmen zur Verbesserung des Datenschutzes und der Datensicherheit eingeführt. So wurden zum Beispiel Maschinen aus der Produktion, die bisher eine Netzwerkschnittstelle besaßen, vom Firmennetz und dem Internet getrennt.

Zudem werden die Mitarbeiter durch den Datenschutzbeauftragten der Firma geschult und speziell für die Gefahren durch Social Engineering sensibilisiert. Durch monatliche E-Mails, Hinweise im Intranet und weitere Schulungen soll die Wachsamkeit der Mitarbeiter auf einem hohen Niveau gehalten werden.

Das Projekt steht beispielhaft dafür, wie ein mittelständisches produzierendes Unternehmen die firmeninterne Sicherheit erhöhen kann.

Edelstahl Rosswag GmbH | Pfinztal
www.edelstahl-rosswag.de

2. Preis 2009: SAP AG

Projekt Destination: Security@SAP – globale Awareness-Kampagne

Die Awareness-Kampagne „Destination: Security@SAP“ hatte zum Ziel, das Sicherheitsbewusstsein der SAP-Mitarbeiter zu stärken. Inhalte waren die SAP Security Policy und die wichtigsten dazugehörigen Sicherheitsstandards.

Dies geschah erstmalig spielerisch in Form eines Online-Trainings, das allen Mitarbeitern im Mitarbeiterportal vorgestellt wurde. Bei erfolgreicher Teilnahme konnten die Mitarbeiter attraktive Preise gewinnen. Als Schauplatz für die Vermittlung der Sicherheitsinhalte wurde das Thema „Flughafen“ gewählt, da Flughäfen mit vielen Sicherheitsvorkehrungen verbunden sind. Auf den Postern, die die Kampagne vorstellten, wurde eine Stewardess oder ein Steward abgebildet. Als Flugblatt, das an jeden Mitarbeiter verteilt wurde, wurde eine Bordkarte erstellt und der Eröffnungsfilm, der zur Teilnahme an der Kampagne einlädt, stellt eine Stewardess dar, die auf typische fehlende Sicherheitsvorkehrungen von Mitarbeitern (insbesondere in Flugzeugen) hinweist.

Insgesamt ist die Kampagne ein gelungenes Beispiel dafür, dass Informationsschutz nicht mit erhobenem Zeigefinger erfolgen muss, sondern durchaus auch auf spielerische Weise und mit einem gewissen „Augenzwinkern“ erfolgen kann.

SAP AG | Walldorf
www.sap.de


I-SAFET
Sicherheitsforum Baden-Württemberg
2. Preis 2009
SAP AG
Walldorf


ronik
Sicherheitsforum
Baden-Württemberg
2. Preis 2009

2. Preis 2009: EnBW Kernkraft GmbH

Projekt Definition und Anwendung eines IT-Sicherheits-Zonenmodells

Die IT-Systeme des Preisträgers sind durch ihre Vielseitigkeit, stark unterschiedlich geprägte Schutzbedarfe und durch den Einsatz spezifischer Lösungen gekennzeichnet. Während in Teilen der Bürokommunikation ein großes Kommunikationsaufkommen zwischen den drei Unternehmensstandorten besteht, werden – auch aus Gründen der IT-Sicherheit – anlagennahe IT-Systeme am jeweiligen Standort autark betrieben.

Das IT-Sicherheitskonzept gründet sich im Kern auf die drei Dokumente „IT-Sicherheitsmanagement", „IT-Sicherheitsleitlinie" und „IT-Sicherheitskonzept" zur Beschreibung der Vorgaben, Regelungen, Richtlinien und Organisationsstrukturen zur Erreichung und Wahrung der Sicherheitsziele. Als Teil des standortübergreifenden Managementsystems wurde auch ein IT-Sicherheitsprozess erarbeitet und eingeführt, um die Verantwortlichkeiten und Prozessabläufe genau zu definieren und den Organisationseinheiten zuzuordnen.

Das Zonenmodell sieht vier anhand des Schutzbedarfs gestufte IT-Sicherheitszonen vor. Die inneren Zonen beinhalten die IT-Systeme der technischen IT (Leittechnik) mit überwiegend sehr hohem beziehungsweise hohem Schutzbedarf, während in den äußeren Zonen die IT-Systeme mit überwiegend mittlerem Schutzbedarf angesiedelt sind (zum Beispiel Bürokommunikation). Dieses IT-Zonenkonzept wurde 2007 im Rahmen einer Betriebsbewertung durch die Internationale Atomenergiebehörde (IAEA) als vorbildlich gewürdigt und dient heute als Referenz für kerntechnische Anlagen weltweit. Das Modell zeigt einen strukturierten, wirkungsvollen und wirtschaftlich vertretbaren Ansatz auf, der auch in mittelständischen Unternehmen umgesetzt werden könnte, um Know-how und sensible Daten entsprechend ihres Schutzbedarfs zu sichern.

EnBW Kernkraft GmbH
Kernkraftwerk Neckarwestheim
www.enbw.com

1. Preis 2007: ZF Friedrichshafen AG

Projekt Awareness-Kampagne zum Informationsschutz

Die während des gesamten Jahres 2007 laufende Kampagne hatte vor allem die Sensibilisierung der Mitarbeiter zu allen Aspekten des Informationsschutzes zum Ziel. Weltweit wurden rund 2.000 Führungskräfte und rund 54.000 Mitarbeiter mit verschiedensten Medien – unter anderem Plakate, Mitarbeiterzeitungen, Videos und Fragebogen – angesprochen. Informationen zum Know-how-Schutz für neue Mitarbeiter, die Bestellung von Informationsschutzbeauftragten in allen Unternehmensbereichen und ein Benchmarking innerhalb des Unternehmens rundeten die Kampagne ab. Das Projekt wurde nach Jahresende unter Einsatz eines speziellen „Security-AwarenessMonitor"-Programms einer Evaluation unterzogen.

ZF Friedrichshafen AG | Friedrichshafen
www.zf.com


security consulting
Lassen Sie Ihre Brieftasche
ine Freiheit."
n von Humboldt
1. Preis 2007


Lassen Sie Ihre Brie
liegen?
ist keine Freiheit."

2. Preis 2007: Mercedes-AMG GmbH

Projekt Fremdhardwareerkennung im LAN

Projektziel war die Erkennung, Lokalisierung und – bei Bedarf – Abwehr von Fremdgeräten externer Partner oder Dienstleister im unternehmensinternen Rechnernetzwerk. Das hierfür geschaffene, arbeitsökonomisch ausgestaltete System ist in der Lage, allen nicht ausdrücklich zugelassenen Endgeräten wie Notebooks oder WLAN-Geräten den Zugriff auf das Netzwerk zu verwehren. Daten können nicht mehr unbemerkt ausspioniert, gelöscht oder manipuliert werden. Geheime Produktentwicklungen und unternehmensinterne Passworte sind vor unerwünschtem Zugriff gesichert.

Mercedes-AMG GmbH | Affalterbach
www.mercedes-amg.com

2. Preis 2007: Secorvo Security Consulting GmbH mit den Partnern Südpol. Die Agentur. und T-Systems Enterprise Service GmbH

Projekt Security-Awareness-Kampagne „Mission Security“

Bei dieser Kampagne, die von März bis Juli 2006 bei T-Systems durchgeführt wurde, ging es nicht allein um die Vermittlung von Wissen zum Informationsschutz. Die Mitarbeiter sollten vor allem darin bestärkt werden, Informationen auch gegen etwaige Widerstände zu schützen und sich richtig zu verhalten. Diese Aufgabe erledigte „James Bit“, ein fiktiver T-Systems-Mitarbeiter mit einer eigenen Biographie. Er stand als Leitfigur im Mittelpunkt der Kampagne. Es ist ein psychologisch einfühlsam aufbereitetes Konzept gelungen, das das Bewusstsein der Mitarbeiter für das Thema Informationssicherheit schärfen kann.

Secorvo Security Consulting GmbH | Karlsruhe
www.secorvo.de

T-Systems Enterprise Service GmbH
Leinfelden-Echterdingen | www.t-systems.com

Südpol. Die Agentur. | Niedereschach


IDEEN
Karlsruhe –
Messen und Kongr


Systems

2. Preis 2007: Fiducia IT AG

Projekt Security-Awareness-Kampagne

Das Projekt, das im Jahr 2007 während eines Zeitraums von drei Monaten durchgeführt wurde, zielt auf eine Verbesserung des persönlichen Sicherheitsbewusstseins bei den Mitarbeitern, auf die Etablierung eines höheren Sicherheitsstandards durch die Einübung bestimmter Handlungsweisen und auf die Erweiterung und Festigung des Wissens zum Thema Informationssicherheit ab. Mit einem interaktiven IT-Wissensquiz, dem Einsatz von Mitarbeitern als sogenannte Testimonials und Filmen, bei denen Mitarbeiter als Hauptakteure auftreten, ist es gelungen, das Thema Sicherheit spielerisch und ohne erhobenen Zeigefinger zu vermitteln.

Fiducia IT AG | Karlsruhe
www.fiducia.de

Mitglieder im Sicherheitsforum

Allianz für Sicherheit in der Wirtschaft Baden-Württemberg e. V.
» **www.asw-bw.com**

Baden-Württembergischer Handwerkstag
» **www.handwerk-bw.de**

Baden-Württembergischer Industrie- und Handelskammertag
» **www.bw.ihk.de**

Daimler AG
» **www.daimler.com**

EnBW Energie Baden-Württemberg AG
» **www.enbw.com**

Karlsruher Institut für Technologie
» **www.kit.edu**

Landesamt für Verfassungsschutz Baden-Württemberg
» **www.verfassungsschutz-bw.de**

Landeskriminalamt Baden-Württemberg
» **lka.polizei-bw.de**

Baden-Württemberg

Landesverband der Baden-Württembergischen Industrie e. V.
» www.lvi.de

Ministerium für Inneres, Digitalisierung und Migration Baden-Württemberg
» im.baden-wuerttemberg.de

Ministerium für Wirtschaft, Arbeit und Wohnungsbau Baden-Württemberg
» wm.baden-wuerttemberg.de

Robert Bosch GmbH
» www.bosch.de

SAP AG
» www.sap.com

Steinbeis-Stiftung
» www.steinbeis.de

VDMA Baden-Württemberg
» www.vdma.org

Sicherheitsforum Baden-Württemberg
» www.sicherheitsforum-bw.de

Sicherheitsforum
Baden-Württemberg
Die Wirtschaft schützt ihr Wissen

Impressum

Sicherheitsforum Baden-Württemberg
Willy-Brandt-Str. 41
70173 Stuttgart

Fon: +49 711 231-4
Fax: +49 711 231-3599
E-Mail: poststelle@im.bwl.de

Titelbild: TippaPatt/Shutterstock.com
Bilder Inhalt: S. 7: Steinbeis, S. 11: Sicherheitstechnik Sancak e.K., S. 12: Schweickert Netzwerktechnik GmbH, S. 15: Robert Bosch GmbH, S. 16–36: Messe Stuttgart/Fotodesign Zuckerfabrik, S. 39–44: Landesamt für Verfassungsschutz, S. 47–52: Tom Kohler

Satz: www.steinbeis-edition.de | 205421-2019-03

www.sicherheitsforum-bw.de