AUSGABE 9

SICHERHEIT. DAS FACHMAGAZIN.

SICHERHEIT AUF DEN PUNKT GEBRACHT.

SIUS Consulting

KOMPETENZPARTNER

SICHERHEIT.
DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.

SICHERHEIT. DAS FACHMAGAZIN.

bietet kleinen und mittelständischen Unternehmen, Behörden und Organisationen bedeutendes und praxisnahes Wissen. Mit konkreten Schritt-für-Schritt-Anleitungen, individuell anpassbaren Musterdokumenten und Formularen, praktischen Handlungsempfehlungen sowie innovativen Tools und Werkzeugen verspricht Ihnen SICHERHEIT. Das Fachmagazin. einen einzigartigen Mehrwert.

DOWNLOADS

Alle Ausgaben von SICHERHEIT. Das Fachmagazin. enthalten nützliche und wissenswerte Downloads. Diese finden Sie auf unserer Homepage unterhalb der jeweiligen Ausgabe.

SECURITY-SERVICE-CENTER

Mit unserem Security-Service-Center bieten wir Ihnen einen attraktiven Mehrwert. Sollten Sie zu einzelnen Artikeln nähere Informationen benötigen, Rückfragen haben oder ggf. auf der Suche nach kompetenter Fachexpertise sein, stehen Ihnen unsere Experten jederzeit gerne zur Verfügung.

Telefon: +49 (0) 30 / 700 36 96 5
E-Mail: redaktion@sicherheit-das-fachmagazin.de

KOSTENFREI & UNVERBINDLICH

Warum ist SICHERHEIT. Das Fachmagazin. für Sie kostenfrei erhältlich?

Sicherheit hat in vielen Unternehmen, Behörden und Organisationen einen eher nebensächlichen Stellenwert, kaum personelle Ressourcen und/oder entsprechendes Budget. Durch das kostenfreie Angebot gelingt es uns, aktuelle (Sicherheits-)Themen, Trends und Entwicklungen mit unseren Zielgruppen zu teilen, unabhängig davon, ob das nötige Budget für ein Abonnement aufgebracht werden kann.

Wie finanziert sich SICHERHEIT. Das Fachmagazin.?

Das Magazin finanziert sich durch erkennbare Werbeanzeigen, Kompetenzpartner und sog. Affiliate-Links im Rahmen des Amazon Partnerprogramms. Unabhängig davon gilt bei der redaktionellen Arbeit jedoch stets der Grundsatz einer neutralen und seriösen Informationsvermittlung: „Werbung bleibt Werbung, Artikel bleibt Artikel!“

Erfahren Sie mehr unter www.sicherheit-das-fachmagazin.de/transparenzhinweis

GENDERHINWEIS: *Aus Gründen der besseren Lesbarkeit wird bei SICHERHEIT. Das Fachmagazin. auf eine geschlechtsneutrale Differenzierung (z. B. Mitarbeiterinnen/Mitarbeiter) verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.*

UNSERE KERNTHEMEN

- Wirtschaftsschutz
- Sicherheitsvorkehrungen
- Krisen- und Notfallmanagement
- Security Awareness
- Reisesicherheit

E-PAPER

SICHERHEIT. Das Fachmagazin. als ePaper bringt Ihnen alle Vorzüge eines gedruckten Magazins auf Ihren Bildschirm: ob zu Hause oder unterwegs, im Büro oder im Urlaub – auf Ihrem PC, Tablet und Smartphone.

Ihre Vorteile:

› Ressourcenschonend durch nachhaltige Einsparungen beim Verbrauch von Papier, Treibstoff und CO_2

› Komfortable Web-Ansicht mit besonderen Bedienfunktionen oder als Download im klassischen PDF-Format

NUTZEN SIE DIE MÖGLICHKEITEN EINES STUDIENPRAKTIKANTEN AUS DEM BEREICH „SICHERHEITSMANAGEMENT“

Zum Wintersemester 2020 (ab Oktober) suchen wieder bundesweit Studenten aus den Studiengängen „Sicherheitsmanagement“ einen Praktikumsplatz im betrieblichen, gewerblichen oder kommunalen Umfeld der Sicherheit.

Für Unternehmen und Institutionen bietet dies die Möglichkeit, sicherheitsrelevante Themen von erfahrenen Studenten ausarbeiten oder aktiv begleiten zu lassen. Aus eigener Erfahrung können wir Ihnen nur ans Herz legen, nicht davor zurückzuschrecken, einen Studenten für einen begrenzten Zeitraum zu beschäftigen. Ein Studienpraktikant ist dankbar für die praktischen Einblicke und Erfahrungswerte, die geboten werden.

„Kleinere“ Sicherheitsaufgaben gibt es viele, wie beispielweise:

- Verschriftlichung von (Sicherheits-)Prozessen und (Sicherheits-)Konzepten
- Erstellung von Richtlinien, Checklisten, Handlungsanweisungen
- Durchführung von Preis- und Marktrecherchen (Anbietervergleich)
- Prüfung und Optimierung von sicherheitsrelevanten (Dienst-)Anweisungen
- Unterstützung/Zuarbeiten im Rahmen kleinerer Sicherheitsprojekte
- Erstellung/Überarbeitung des Intranet-Auftritts der Sicherheitsabteilung

Je nach Interessenlage kann jede Abteilung des Unternehmens, die Berührungspunkte zum Thema „Unternehmenssicherheit“ hat, themenspezifisch eingebunden und durch den Studenten für eine gewisse Zeit begleitet werden (z. B. Arbeitssicherheit, Brandschutz, Facility Management, Datenschutz, IT-Sicherheit etc.), um so die sicherheitsspezifischen Zusammenhänge und Denkweisen der einzelnen Fachbereiche näher kennenzulernen.

Ziel des Praktikums soll es sein, bisher erworbenes theoretisches Fachwissen auf die Praxis zu beziehen und berufliche Erfahrungen zu sammeln. Dabei ist ein wesentlicher Bestandteil, die Sicherheitsanforderungen eines Unternehmens auch im wirtschaftlichen Kontext zu verstehen und damit einhergehend etwaige Frage- und Problemstellungen für das Erstellen der Studienarbeit mitzunehmen.

HOCHSCHULEN/UNIVERSITÄTEN MIT STUDIENGÄNGEN IM BEREICH „SICHERHEITSMANAGEMENT“

Hochschule für Wirtschaft und Recht Berlin • Universität Siegen
Hochschule der Polizei Hamburg • NBS Northern Business School Hamburg
Hochschule Magdeburg-Stendal • Technische Hochschule Ingolstadt
Hochschule für Öffentliche Verwaltung Bremen • Hochschule Furtwangen

GRUNDSÄTZLICHE REGELN FÜR DEN WIRTSCHAFTSSCHUTZ

Die zunehmende Globalisierung und die internationale Spitzenstellung deutscher Unternehmen wecken nicht nur bei Konkurrenten Begehrlichkeiten, sondern auch bei fremden Staaten. Diese Begehrlichkeiten bergen erhebliche Risiken, denn alle materiellen und unternehmerischen Werte sind nur dann etwas wert, wenn sie effektiv vor Ausspähung, Abwanderung oder Sabotage geschützt werden.

Wirtschaftsschutzmaßnahmen im Unternehmen zu etablieren, bedeutet informationstechnische Maßnahmen mit baulichen, technischen, personellen und organisatorischen Aspekten und Maßnahmen zu verknüpfen, um die zukünftige Wettbewerbsfähigkeit aufrechtzuerhalten. Daher kann man grundsätzliche Aussagen treffen, die jedes Unternehmen und jede Organisation im neuen Jahrzehnt beachten, betrachten und berücksichtigen sollte!

NICHTS TUN HILFT NICHT! SCHÜTZEN SIE IHR UNTERNEHMEN!

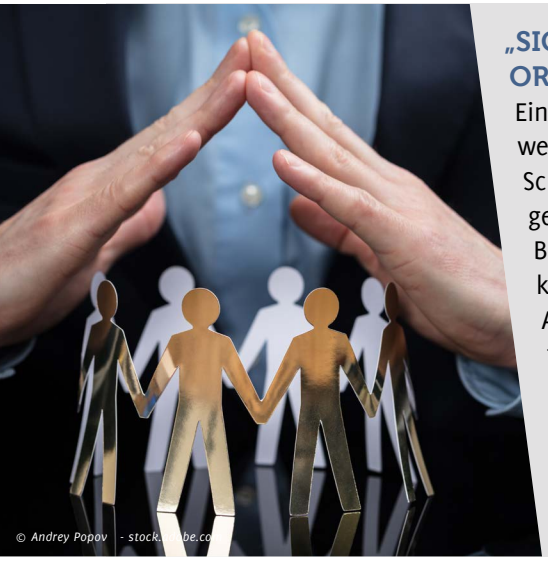
Sicherheits- und Wirtschaftsschutzmaßnahmen sind in den meisten Fällen nicht gesetzlich verankert, daher ist hier Eigeninitiative gefordert und Kreativität gefragt. Gerade kleine und mittelständische Unternehmen oder auch Institutionen verfolgen oftmals die Denkweise, „Warum sollten wir für Kriminelle wichtig sein?“ oder „Was ist bei uns schon zu holen?“. Doch statistische Zahlen belegen jedes Jahr aufs Neue, dass diese Sichtweise falsch ist. Denn gerade kleine und mittelständische Unternehmen sind das Rückgrat der deutschen Wirtschaft und stehen daher durchaus im Fokus krimineller Vereinigungen oder fremder Staaten.

IDENTIFIZIEREN – BEWERTEN – SCHÜTZEN …

… lautet das grundsätzliche Motto, nach dem Wirtschaftsschutzmaßnahmen im Unternehmen aufgebaut werden sollten.

1. Schutzziel(-e) definieren (Kernprozesse und Know-how)
2. Risiken identifizieren (insb. Daten und Informationen)
3. Risikoursachen herausarbeiten
4. Anfälligkeiten zuordnen (inkl. Infrastruktur und Prozesse)
5. Sicherheitsmaßnahmen ableiten, implementieren und aufrechterhalten

©Ruediger Rau - stock.adobe.com



© Andrey Popov - stock.adobe.com

„SICHERHEIT“ SOLLTE NICHT NUR AUS GRÜNDEN DER ORGANISATIONSHAFTUNG ZUR CHEFSACHE ERKLÄRT WERDEN!

Eine Sicherheitskultur im Unternehmen sollte immer von oben nach unten gelebt werden, denn dies führt systematisch und ganzheitlich gedacht zur Erfolgsabsicherung. Schutzmaßnahmen können nur dann effektiv wirken, wenn alle Mitarbeiter einbezogen werden und auch das Signal erhalten, dass dieses Thema einen essenziellen Baustein im unternehmerischen Denken und Handeln einnimmt. Gelebte Sicherheit kann auch einen positiven Aspekt auf die Außenwirkung entfalten und ggf. bei Angebotsabgaben und Ausschreibungen zu erheblichen Wettbewerbsvorteilen führen.

Und „NEIN“: Sicherheit kostet nicht nur Geld. Denn die Mehrkosten für den Umgang mit kriminellen Übergriffen, Sabotageakten, Prozessausfällen, Rechtsstreitigkeiten, Imageschäden, Reputationsverlusten etc. sind i. d. R. langfristig betrachtet wesentlich höher.

> SICHERHEIT IST NICHT ALLES,
> ABER OHNE SICHERHEIT IST ALLES NICHTS!

HILFE HOLEN IST NICHT SCHWER, SICHERHEITSMÄNGEL WIEGEN MEHR!

In vielen Unternehmen und Institutionen existiert kein ausreichendes Know-how, um den heutigen Sicherheitsanforderungen gerecht zu werden. Natürlich kann „Jeder" Sicherheitsmaßnahmen planen und konzipieren, aber oftmals ist dies dann weder ganzheitlich noch von Anfang bis Ende oder außerhalb der regulären Zeiten und Prozesse gedacht. Daher kann es durchaus ein Mehrwert sein, sich in einigen Bereichen fachliche Unterstützung hinzuzuziehen, um den Bedarf ganzheitlich, nachhaltig und lösungsorientiert zu planen. Dies fängt von baulichen Planungen (Neubau/Erweiterung/Umbau etc.) an und geht über technische Systeme (Zutrittskontrolle, Videoüberwachung, Einbruchmeldeanlagen etc.) bis hin zur externen Sicherheitsdienstleistung, die oftmals nach dem „Billigbieterprinzip" eingekauft wird, ohne dass hier eine professionelle und serviceorientierte Arbeit geleistet wird, die auch einen echten und konkreten Mehrwert darstellt.


©oatawa - stock.adobe.com


©Expensive - stock.adobe.com

MANCHMAL IST ES BESSER, EBEN DOCH ETWAS ZU SAGEN

Sicherheitsvorfälle kommen in allen noch so gut gesicherten Bereichen vor – bei (Sicherheits-)Behörden, in Justizvollzugsanstalten, in Unternehmen und im Privathaushalt. Oftmals werden Vorfälle oder das Verdachtsmoment aus Scham, Unwissenheit oder aus Angst vor Konsequenzen oder Reputationsverlust verschwiegen und „unter den Teppich gekehrt". Doch gerade dies ermöglicht Tätern das gleiche Vorgehen an anderer Stelle – denn nur aus Fehlern können wir und auch Andere lernen. Daher empfiehlt sich eine enge und präventive Zusammenarbeit mit den Sicherheitsbehörden, interne Meldeketten sowie die Sensibilisierung für Sicherheitsrisiken jedweder Art. Gerade bei Spionageverdachtsfällen unterstützt u. a. der Verfassungsschutz vertraulich und kostenfrei mit praxisgerechter und fachkundiger Unterstützung. Zum Teil gibt es hier auch kostenfreie Angebote bei der Initiierung geeigneter Sicherheitsmaßnahmen.

SICHERHEIT NACHHALTIG LEBEN

Hierzu zählen viele Faktoren, die nicht immer augenscheinlich zur Sicherheit zählen aber ihre Wirkung auch in diesem Bereich entfalten. Dies betrifft beispielsweise die Motivation und Loyalität von Mitarbeitern ebenso wie die Informationssparsamkeit insbesondere im firmenfremden Umfeld. Sicherheitsstandards müssen jederzeit funktionieren, daher ist das stete Erinnern und Wachrütteln der Mitarbeiter entscheidend. Sensibilisierungsmaßnahmen und Security-Awareness-Kampagnen können genutzt werden, um Mitarbeiter fortlaufend für das Thema zu sensibilisieren sowie entsprechend zu mobilisieren.

In regelmäßigen Abständen müssen Prozesse und Konzepte überprüft und angepasst werden, um stets auf dem Laufenden zu bleiben und aktuellen Bedrohungsszenarien entgegenzuwirken. Sicherheit sollte niemals Routine werden, denn Gewohnheiten und routinierte Abläufe führen dazu, dass Unachtsamkeit und Unbekümmertheit einen Nährboden haben.

©gustavofrazao - stock.adobe.com

ARGUMENTE UND HILFESTELLUNGEN FÜR DEN AUFBAU EINES NOTFALL- UND KRISENMANAGEMENTS

Jede außergewöhnliche und komplexe Abweichung von den alltäglichen Geschäftsvorgängen und -prozessen kann Verantwortliche schnell vor große Herausforderungen stellen. Wenn es sich in einem solchen Fall auch noch um eine Notfall- oder Krisensituation handelt, die beispielsweise für den Geschäftsbetrieb, das öffentliche Ansehen oder gar die Existenz des Unternehmens von entscheidender Bedeutung ist, dann ist ein souveränes Notfall- und Krisenmanagement unabdingbar.

In vielen Unternehmen und Institutionen fehlt oftmals ein solches Notfall- und Krisenmanagementsystem, was u. a. daraus resultiert, dass es – mit Ausnahme einiger Branchen – an den entsprechenden rechtlichen Grundlagen fehlt. Daher liegen hier die Argumente „Eigenverantwortung" und „unternehmerische Weitsichtigkeit" klar auf der Hand.

> „EINE KRISE IST GRUNDSÄTZLICH AUSSERGEWÖHNLICH UND KANN WEITREICHENDE SCHÄDIGENDE FOLGEN FÜR DIE BETROFFENEN HABEN. UM KRISEN SYSTEMATISCH UND STRUKTURIERT BEWÄLTIGEN ZU KÖNNEN, IST EIN NOTFALL- UND KRISENMANAGEMENT UNABDINGBAR.

Gerade in „guten Zeiten" sollte man sich mit realistischen Risikoszenarien beschäftigen, die zu einer Notfall- oder gar Krisensituation im Unternehmen führen können. Die möglichen Notfall- und Krisenrisiken sollten dabei nicht allein die Gefährdung von Leib und Leben sowie Sach- und Umweltschäden berücksichtigen, sondern auch damit verbundene oder durch Ereignis X einhergehende unternehmerische Existenzrisiken. Eine Notfall- oder Krisensituation kann sich bereits aus vermeintlich „harmlosen" (Ursprungs-)Ereignissen ergeben und hierbei relativ schnell eine unkalkulierbare (Eigen-)Dynamik entwickeln, wie die nachfolgende Grafik verdeutlichen soll:

SCHWELLENWERTE / ESKALATIONSSTUFEN

	! STÖRUNG !	!! NOTFALL !!	!!! KRISE !!!
ERLÄUTERUNG	Kurzfristige Beeinträchtigung oder kurzzeitiger Ausfall von Prozessen oder Ressourcen mit nur geringem Schaden.	Länger andauernder Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden.	Im Wesentlichen auf das Unternehmen begrenzter verschärfter Notfall, der die Existenz des Unternehmens bedroht oder die Gesundheit oder das Leben von Personen beeinträchtigt.
BEISPIEL			

Je nach Lage sowie Reaktions- und Interventionsgeschwindigkeit kann sich der Ablauf eines Ereignisses schrittweise von einer Störung, zu einem Notfall bis hin zu einer Krise mit existenzbedrohendem Ausmaß entwickeln!

Angesichts der (Eigen-)Dynamik einer Krise ist diese meist kaum vorhersehbar. Dadurch sind auch Maßnahmen und Handlungsanweisungen stets nur ein grober Rahmen, der im Vorfeld dennoch genauestens definiert werden sollte, um im Ereignisfall ein Regelwerk zu haben, an dem man sich orientieren kann.

ARGUMENTE FÜR EIN NOTFALL- UND KRISENMANAGEMENT

Das Ziel und damit auch die Argumente für den Aufbau und die Einführung eines Notfall- und Krisenmanagements können beispielsweise lauten:

- Schäden frühzeitig einzudämmen bzw. einzugrenzen,
- weiteren Eskalationen bzw. Folgeschäden entgegenzuwirken,
- Schadensauswirkungen bzw. Schadensausbreitungen zu minimieren,
- die Ausbreitung des Notfalls bzw. der Krise auf andere Bereiche/Dritte zu verhindern,
- ein gewisses Maß an Übersicht, Kontrolle und Steuerung wiederzuerlangen und
- mit externen Einflussfaktoren (Presse, Medien, Öffentlichkeit) angemessen umzugehen.

Im Ereignisfall kann es essentiell sein, sich seiner unternehmerischen, aber auch persönlichen Fähigkeiten, Verantwortungen, Zuständigkeiten und vor allem auch Grenzen vollends bewusst zu sein.

Es kann fatal sein, sich solcher Fakten erst im Ernstfall bewusst zu werden. Auch hier hilft ein strukturiertes und systematisch aufgebautes Notfall- und Krisenmanagementsystem bereits im Vorfeld, die Resilienz (Widerstandsfähigkeit) zu stärken und im Ereignisfall strukturierter, vorausschauender und professioneller zu agieren.

DIE FÄHIGKEITEN IM NOTFALL- UND KRISENMANAGEMENT BESTEHEN AUS 3 BAUSTEINEN:

Um das Thema „Notfall- und Krisenmanagement“ aktiv in die Praxis zu überführen, sollten regelmäßige theoretische Schulungen und Unterweisungen sowie praktische Übungen, Workshops oder Planspiele durchgeführt werden, um das Thema ganzheitlich zu verdeutlichen und die Denkweisen der handelnden Akteure kontinuierlich zu erweitern. Denn eine reale Notfall- oder Krisensituation stellt insbesondere die handelnden Akteure vor enorme physische und psychische Herausforderungen, was u. a. den Faktoren Stress, Zeitdruck, Verantwortungsdruck, Entscheidungsdruck etc. geschuldet ist. ›››

HILFESTELLUNGEN FÜR EIN NOTFALL- UND KRISENMANAGEMENT

Für den Aufbau und Betrieb eines Notfall- und Krisenmanagements existieren eine Reihe von Hilfestellungen/Orientierungshilfen in Form von allgemeinen und branchenspezifischen Standards, Normen und „Technischen Regeln“, wie beispielsweise (nicht abschließend):

- DIN CEN/TS 17091: Krisenmanagement - Strategische Grundsätze
- DIN ISO 31000: Risikomanagement
- DIN EN ISO 22301: Business Continuity Management System
- BSI-Standard 100-4: Notfallmanagement
- Wirtschaftsgrundschutz Standard 2000-3: Notfall- und Krisenmanagement
  - Wirtschaftsgrundschutz Standard ÜA3: Notfallmanagement
  - Wirtschaftsgrundschutz Standard ÜA4: Krisenmanagement
  - Wirtschaftsgrundschutz Standard ÜA6: Krisenkommunikation

Branchenspezifisch (beispielhaft):

- IT-Sicherheitsgesetz (KRITIS)
- Störfall-Verordnung (12. BImSchV)
- DIN EN 15975-1: Krisenmanagement in der Trinkwasserversorgung
- DIN EN 15975-2: Risikomanagement in der Trinkwasserversorgung
- Mindestanforderungen an das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht

Bild links: Beispiel einer Krisenstabsrahmenübung (SIUS Consulting)

SICHERHEIT IST UNSERE STÄRKE

UNSERE LEISTUNGEN

- SICHERHEITSBERATUNG
- SICHERHEITSKONZEPTIONEN
- REISESICHERHEIT IM AUSLAND
- EXT. SICHERHEITSMANAGEMENT
- KRISEN- UND NOTFALLMANAGEMENT
- BUSINESS-CONTINUITY-MANAGEMENT
- SECURITY-AWARENESS VIA E-LEARNING

Besuchen Sie uns online:
www.sius-consulting.com

SIUS
Consulting

WARUM DEUTSCHE AUSLANDSVERTRETUNGEN FÜR REISENDE MITARBEITER WICHTIG WERDEN KÖNNEN?

Viele Reisende – ob geschäftlich oder privat – wissen nicht, wohin man sich wenden kann, wenn im jeweiligen Reiseland ein Problem auftritt. Zur guten Fürsorge- und Sorgfaltspflicht von Unternehmen und Institutionen zählt daher auch, dass Reisende und entsandte Mitarbeiter diesbezüglich aufgeklärt werden.

Die deutschen Auslandsvertretungen – bestehend aus Botschaften, Generalkonsulaten oder Konsulaten – können als „Augen, Ohren und Stimme“ Deutschlands im Ausland bezeichnet werden. Sie unterstehen den Weisungen des Auswärtigen Amtes und vertreten somit die Bundesrepublik, wahren deutsche Interessen und schützen deutsche Bürger im Gastland.

TÄTIGKEITEN DER AUSLANDSVERTRETUNGEN IM GASTLAND

Mitarbeiter können sich auf einer Auslandsreise jederzeit an eine der deutschen Auslandsvertretungen wenden, auch wenn sich die Aufgaben der Botschaften und Konsulate unterscheiden.

AUFGABEN DER BOTSCHAFTEN:

Die Botschaften fördern politische Beziehungen, Wirtschaftsinteressen, wirken bei der Sozial-, Landwirtschafts- und Entwicklungspolitik mit und fördern die internationale Zusammenarbeit in Forschung und Technologie. Sie informieren die Bundesrepublik über die Verhältnisse des Gastlandes und seiner Regierung. Der Botschafter repräsentiert als Vertreter des Bundespräsidenten die Bundesrepublik Deutschland im Gastland. In Ländern, mit denen Deutschland in verteidigungspolitischen Fragen zusammenarbeitet oder die aus verteidigungspolitischer Sicht von besonderem Interesse sind, ist der Botschaft zusätzlich ein Militärattaché zugeordnet.

AUFGABEN DER GENERALKONSULATE UND KONSULATE:

Generalkonsulate und Konsulate haben einen regional begrenzten Amtsbezirk. Ihr Aufgabenspektrum ist die kulturelle Zusammenarbeit und vor allem das Rechts- und Konsularwesen sowie die Öffentlichkeitsarbeit. Auch Aufgaben deutscher Gerichte, Notare und Kommunalbehörden werden durch die Konsularbeamten für im Ausland lebende Deutsche übernommen. Die politischen Beziehungen sind hingegen den Botschaften vorbehalten. Deutsche Bürger können Rat und Beistand in Notsituationen sowie Auskünfte verschiedener Art bekommen.

Reisende und entsandte Mitarbeiter sollten dazu angehalten werden, sich in die Liste des Auswärtigen Amtes „zur elektronischen Erfassung von Deutschen im Ausland“ registrieren zu lassen (https://elefand.diplo.de), um im Not- oder Krisenfall rechtzeitig und fortlaufend relevante Informationen zur Lage zu erhalten.

UNSER TIPP

Die Auslandsvertretungen stehen zudem deutschen Unternehmen bei ihren Aktivitäten im Gastland zur Seite. Über die deutsche Auslandsvertretung können Unternehmen oder Institutionen im Ausland an die regionalen Sicherheitsberater herantreten, um die Sicherheitsmaßnahmen von Gebäuden und Personen planen zu können. Die regionalen Sicherheitsberater sind speziell ausgebildete Sicherheitsbeamte der Bundespolizei mit dem Einsatzziel, mit ihrer polizeilichen Expertise die Sicherheitsarchitektur an den Botschaften/Konsulaten/Auslandsvertretungen zu verbessern und die Leitungen in Sicherheitsfragen zu beraten. Sie geben Handlungsempfehlungen in sämtlichen Bereichen der personellen und materiellen Sicherheit sowie in der Krisenvorsorge und halten Kontakt zu Polizei- und Sicherheitsbehörden des Gastlandes sowie zu Sicherheitsfirmen.

WANN SICH MITARBEITER AN DIE AUSLANDSVERTRETUNGEN WENDEN KÖNNEN?

Die Auslandsvertretungen unterstützen deutsche Staatsbürger, die in Not geraten sind, leisten Krisenvorsorge und übernehmen behördliche und notarielle Funktionen für im Ausland lebende Deutsche. Sollten deutsche Staatsbürger

- verhaftet worden sein,
- rechtliche oder gesundheitliche Probleme haben,
- einen Todesfall zu beklagen haben,
- wichtige Dokumente, die zur Ausreise benötigt werden, verloren haben, oder
- einen Dolmetscher benötigen

können sie sich jederzeit an die deutsche Auslandsvertretung wenden. Auch bei finanziellen Problemen kann die Auslandsvertretung unterstützen. Sollte im Reiseland keine Auslandsvertretung vorhanden sein, unterstützen in der Regel auch Botschaften anderer EU-Nationen.

„DIE KONTAKTDATEN DER AUSLANDSVERTRETUNG IM REISELAND SOLLTEN IN JEDEM FALL AUF DIE NOTFALLKARTE BZW. CHECKLISTE DER WICHTIGEN ANSPRECHPARTNER AUF REISEN, SO KÖNNEN IM NOTFALL ABLÄUFE BESCHLEUNIGT WERDEN.

Reisende und entsandte Mitarbeiter, sollten sich auf jeden Fall in die Krisenvorsorgeliste des Auswärtigen Amtes eintragen – auch bei kurzzeitigen Reisen. Diese Daten werden an die deutschen Auslandsvertretungen weitergeleitet. Dies führt dazu, dass Personen beispielsweise rechtzeitig über Krisen informiert und in Maßnahmen der Krisenvorsorge und -reaktion einbezogen werden.

KLEINE LÜCKE – GROSSER SCHADEN

PENETRATIONSTESTS ALS BEWERTUNGSTOOL DER IT-SICHERHEIT

Aktenordner waren gestern. Die Digitalisierung hat längst in die Verwaltungs- und Unternehmenspraxis Einzug gehalten. Der technische Fortschritt öffnet viele Chancen für Unternehmen, ihre Arbeitsabläufe zu vereinfachen und effektiver zu gestalten, zügiger auf Marktänderungen zu reagieren – sowie besser mit Kunden und eigenen Mitarbeitern zu kommunizieren. Die Umstellung auf das digitale Zeitalter stellt Unternehmen jedoch auch vor vielfältige Herausforderungen und birgt Risiken für die Unternehmens- und Informationssicherheit.

Mit zunehmender Komplexität von IT-Systemen und Infrastruktur ist das Ziel der Unternehmenssicherheit als Teil des Wertschöpfungsprozesses für das Management ebenso komplexen Bedrohungsphänomenen ausgesetzt wie einem fortschreitenden Wandel unterworfen. Es heißt „Unternehmenssicherheit ist Chefsache“. Doch wie kann das Management bei der rasanten Entwicklung der Informations- und Kommunikationstechnologien und der hohen Dynamik von externen Bedrohungen Systeme und Daten absichern, Risiken bewerten und mögliche Schäden vermeiden? Ein Penetrationstest ist hier nicht das Allheilmittel, kann Führungskräfte und IT-Verantwortliche aber gezielt darin unterstützen, die IT-Sicherheitsorganisation und den Reifegrad von Schutzmaßnahmen im Unternehmen punktuell zu bewerten.

UNTERNEHMENSSICHERHEIT IM WANDEL

Im Zuge der rasanten Digitalisierungsprozesse der letzten Jahre und dem mittlerweile hohen Stellenwert der IT für moderne Unternehmen wird das Sicherheitsmanagement heute zuweilen oftmals auf die IT-Sicherheit im Unternehmen reduziert. Selbstverständlich sind in einem ganzheitlichen Sicherheitskonzept, in dem alle relevanten Gefährdungen und die daraus entstehenden Gegenmaßnahmen betrachtet werden, die klassischen Aspekte der Unternehmenssicherheit, wie beispielsweise Schließ- und Zugangssysteme oder der Wach- und Werkschutz, weiterhin zu berücksichtigen.

DEFINITION PENETRATIONSTEST

Ein **Penetrationstest**, kurz **Pentest**, ist ein umfassender Sicherheitstest aller Bestandteile und Anwendungen eines Netzwerk- oder Softwaresystems mit Mitteln und Methoden, die ein Angreifer (ugs. „Hacker“) anwenden würde, um unautorisiert in das System einzudringen (Penetration). Der Penetrationstest ermittelt und bewertet somit die Verwundbarkeit des zu testenden Systems gegen derartige Angriffe.

Dies ist insbesondere so, weil trotz Rationalisierung und Automatisierung das „papierlose Büro“ in vielen Unternehmen nach wie vor einen unerreichten Idealzustand darstellt. Richtig ist aber auch, dass die Freiheiten der modernen Kommunikations- und Informationsstruktur durch erhöhte Risiken und Unsicherheiten „erkauft“ werden.

NEUE BEDROHUNGSSZENARIEN…

Durch technische Weiterentwicklung und generell besser gesicherte Systeme ist auch das Hacken zunehmend anspruchsvoller geworden, doch mitnichten weniger erfolgreich. Cyberkriminalität hat sich zu einem Geschäft mit eigener Wertschöpfungskette entwickelt. Angriffe sind heute mehr denn je von ökonomischem Denken und politischen Zielen bestimmt.

Diebstahl von sensiblen Personen- und Bankdaten, Industriespionage, Hacking-Angriffe aus dem Internet, Viren, Würmer, Trojaner und Co, oder Phishing-Mails gehören heute längst zum Alltag und werden zukünftig weiter zunehmen. Mit der rasanten Entwicklung der IT-Systeme und der fortschreitenden Vernetzung verändern sich auch die Angriffsmethoden stetig.

LAUT BSI-LAGEBERICHT 2019 STELLEN SCHADPROGRAMME WIE SCHON IN DEN JAHREN ZUVOR DIE GRÖSSTE IT-BEDROHUNG FÜR UNTERNEHMEN UND BEHÖRDEN DAR.

Die Gefahrenpotenziale von Schadsoftware durch längere Betriebsausfälle, Lösegeldzahlungen oder eine langwierige Aufarbeitung der Sachverhalte sind enorm. Weitaus größere Schäden in der Breite sind jedoch den Delikten Datendiebstahl, Computerbetrug, Systembeschädigungen und Computersabotage, Manipulation von Konto- und Finanzdaten sowie der Verletzung geistigen Eigentums zuzuordnen.

Die ohnehin angespannte Sicherheitslage wird zudem durch aktuelle Social Media-Trends, zunehmende Marktdurchdringung von Mobillösungen, fortschreitende Vernetzung von IoT-Geräten und Cloud-Computing verschärft. Zukünftig sind neue Bedrohungen im Rahmen von Künstlicher Intelligenz (KI) zu erwarten.

... DURCH PRÄVENTION ENTGEGENWIRKEN

Mittlerweile hat sich als IT-Sicherheitsstrategie die sogenannte „Assume Breach-Mentalität“ durchgesetzt. Dieser Ansatz unterstellt von Vornherein eine Kompromittierung von Clients durch Malware, die Studien zufolge für ›50% der Angriffe verantwortlich ist. Folgerichtig rücken Maßnahmen in den Fokus, die Angriffe erkennen und deren Ausbreitung auf andere Systeme erschweren. Bei der Absicherung von Systemen und Endgeräten im Unternehmensnetzwerk sowie beim Schutz personenbezogener und sensibler Unternehmensdaten ist Prävention der erste Schritt. Ob über die hausinterne IT-Abteilung oder gar ganze professionalisierte Unternehmenseinheiten wie z. B. Security Operations Center (SOC): das Thema IT-Sicherheit im Allgemeinen und der Sicherheitsstatus der internen IT-Infrastruktur sowie der unternehmenseigenen Datenbestände im Speziellen sind zunehmend im Bewusstsein angekommen. Dennoch kann Computerkriminalität jeden treffen – den Branchenriesen ebenso wie den Mittelständler aus der Kleinstadt. Zunehmend komplexe Systemlandschaften bei gleichzeitig stetiger Weiterentwicklung von Angriffsmethoden und -werkzeugen stellen nach wie vor viele Unternehmen vor die immense Herausforderung, sich immer wieder neu mit Maßnahmen zur Prävention und Reaktion auf kriminelle Handlungen zu wappnen.

WER DIE STETIGE WEITERENTWICKLUNG DER TECHNOLOGIE UND KRIMINELLE ANGRIFFSMUSTER IGNORIERT, WIRD GRAVIERENDE SCHÄDEN NICHT DAUERHAFT VERMEIDEN KÖNNEN. AUF LANGE SICHT WIRD DER FINANZIELLE NUTZEN, DER DURCH DIE VERMEIDUNG ODER MINDERUNG VON POTENZIELLEN SCHÄDEN ENTSTEHT, DIE INVESTITIONEN IN ANGEMESSENE GEGENMASSNAHMEN ÜBERWIEGEN.

ÜBERPRÜFUNG DES SICHERHEITSLEVELS DURCH PENETRATIONSTESTS

Bei den Präventionsmaßnahmen überwiegen in deutschen Unternehmen die Sensibilisierung und Schulung von Mitarbeitern, die Verschlüsselung von Daten und Datenträgern sowie die regelmäßige Identifizierung des Schutzbedarfs von Daten und Systemen (vgl. e-Crime in der deutschen Wirtschaft 2019, KPMG). Ein gutes Mittel zur Überprüfung des Sicherheitslevels aller Systembestandteile und Anwendungen eines Netzwerks sind Penetrationstests. Einen derartigen Test kann jedes Unternehmen aktiv mitgestalten, beispielsweise bei der Auswahl des Testgegenstands und der Testtiefe. Zudem ist es auch möglich, dem Test beizuwohnen und Fragen zu stellen. Der gegenseitige Informationsaustausch ist explizit gewünscht, da somit der Penetrationstester im Gegensatz zum externen Angreifer einerseits im Vorteil ist und bessere Chancen hat, Schwachstellen zu identifizieren, andererseits das „getestete“ Unternehmen nicht außen vor bleibt, sondern den objektiven Blick von außen als zusätzliche Erfahrung verbuchen kann. Insbesondere in Zeiten knapper IT-Budgets können Penetrationstests sogar dabei helfen, Geld zu sparen, indem das begrenzte Budget gezielt für einen bestimmten Testgegenstand und die Beseitigung konkreter Lücken genutzt wird. ›››

NICHT JEDER ANGRIFF KANN ABGEWEHRT ODER GAR VERMIEDEN WERDEN. IM UNTERNEHMENSUMFELD IST ES WICHTIG, AUF ANGRIFFE VORBEREITET ZU SEIN UND EIN GEEIGNETES SICHERHEITSKONZEPT ZU HABEN, UM IM VERDACHTS- ODER BEIM KONKRETEN SICHERHEITSVORFALL MÖGLICHST SCHNELL UND EFFIZIENT REAGIEREN ZU KÖNNEN.

DER PENETRATIONSTEST – WAS ER KANN UND WAS NICHT

Der Begriff „Hacker“ wird in den Medien meist im Zusammenhang mit Computerkriminalität benutzt und ist daher oft stark negativ belegt. Neben diesen sogenannten „Black Hats“, die mit krimineller Energie versuchen, Infrastrukturen und Systeme zu manipulieren, um unerlaubt an Daten zu kommen, gibt es auch noch die „Guten“ (White Hats), die ihre außergewöhnlichen Fähigkeiten und ihr technisches Wissen innerhalb der Gesetze und der Hackerethik einsetzen. Sie werden beispielsweise heute in Unternehmen eingesetzt, um professionelle Penetrationstests durchzuführen. Die Motivation der „White Hats“ ist also eine deutlich andere, die Arbeitsweise jedoch die gleiche wie die der kriminellen „Black Hats“. Der Penetrationstester unternimmt demnach – in Absprache und Zusammenarbeit mit dem Auftraggeber – den kontrollierten Versuch, in ein bestimmtes Computersystem oder Netzwerk einzudringen, um Schwachstellen zu identifizieren. Diese Schwachstellen können dann durch entsprechende Maßnahmen behoben werden, bevor sie von unautorisierten Personen illegal ausgenutzt werden können.

ANGRIFFSSTELLEN VON PENTESTS

Typische Angriffspunkte bei einem Penetrationstest sind Firewalls, Webserver, Remote Access Service (RAS)-Zugänge, Funknetze oder auch einzelne Webanwendungen, um beispielsweise auf Daten zuzugreifen oder sich im Netzwerk auszubreiten. Auf der Seite des Auftraggebers soll somit die Sicherheit der technischen Systeme sowie möglicherweise auch der organisatorischen und personellen Infrastruktur (mit einer Erweiterung auf z. B. Social Engineering oder Red Teaming) erhöht werden. Das Ergebnis eines Penetrationstests sollte vorhandene Schwachstellen auflisten und möglichst konkrete Lösungsvorschlage für deren Beseitigung aufführen.

Dabei ist zu beachten, dass ein Penetrationstest immer nur eine Momentaufnahme darstellt. **Er kann aktuelle Sicherheitslücken identifizieren** oder auch schon länger bekannte, für die noch keine Sicherheitspatches eingespielt bzw. bereitgestellt wurden. **Er kann potenzielle Fehler aufdecken**, die sich aus einer fehlerhaften Bedienung oder Implementierung ergeben. **Es können unzureichend geschützte Systeme erkannt werden**, die besser segmentiert oder gar abgeschottet werden sollten. Dies ist immens wichtig für das Gesamtsicherheitsniveau einer IT-Infrastruktur, da Erfahrungswerte zeigen, dass oft schon eine einzelne kleine Sicherheitslücke für einen Angreifer ausreicht, um gesamte Unternehmensnetzwerke zu kompromittieren.

Im ungünstigsten Fall entsteht unmittelbar nach Abschluss eines Penetrationstests eine neue Schwachstelle, die ein System wiederum verwundbar macht. Die Wirkung eines Penetrationstests ist somit vergänglich, wie schnell, lässt sich kaum objektiv beziffern. Es wird jedoch empfohlen, die Tests in regelmäßigen Abständen zu wiederholen, um langfristig einen guten Sicherheitseindruck über die Systeme zu gewinnen. Dabei gilt: Je höher der Schutzbedarf der Systeme, desto häufiger sollten Penetrationstests durchgeführt werden.

Jedoch ebenso wenig kann ein Penetrationstest die generellen IT-Sicherheitsprüfungen, die beispielsweise im Rahmen von Audits oder Revisionen durchgeführt werden, und auch keine allgemeinen Sicherheitsrichtlinien ersetzen.

„DURCH DIE STÄNDIGE ÄNDERUNG VON BEDROHUNGSMUSTERN UND DIE WEITERENTWICKLUNG VON ANGRIFFSTECHNIKEN KANN KEINE AUSSAGE ÜBER DAS SICHERHEITSNIVEAU DER GEPRÜFTEN SYSTEME IN DER ZUKUNFT ABGELEITET WERDEN, DA EIN PENTEST NUR EINE MOMENTAUFNAHME DARSTELLT.

© kai - stock.adobe.com

DIE PHASEN DES PENETRATIONSTESTS

Ein Penetrationstest gliedert sich in unterschiedliche Phasen, die zeitlich nacheinander ablaufen. Je nach Gliederung werden meist vier oder fünf Phasen unterschieden. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) empfiehlt beispielsweise einen fünfstufigen Prozess.

1. VORBEREITUNG Zu Beginn eines Penetrationstests werden die Ziele des Tests in Zusammenarbeit mit dem Auftraggeber und unter Berücksichtigung der gesetzlichen Bestimmungen sowie der organisatorischen Aspekte geklärt und definiert. Gemeinsam werden die Prüfobjekte und der Testaufbau festgelegt sowie über potenzielle Risiken und entsprechende Notfallmaßnahmen informiert.

2. INFORMATIONSBESCHAFFUNG In der Informationsbeschaffungsphase soll eine möglichst komplette und detaillierte Übersicht über die installierten Systeme inklusive möglicher Angriffspunkte erlangt werden. Die Anzahl der zu untersuchenden Rechner bzw. die Größe des Netzwerks geben in dieser Phase bereits einen Anhaltspunkt für den entsprechenden Zeitbedarf des Penetrationstests.

3. BEWERTUNG Die gewonnenen Informationen werden anschließend einer Bewertung unterzogen, in die die vereinbarten Ziele, die potenzielle Gefährdung und der geschätzte Aufwand einfließen. Auf dieser Basis werden dann die Angriffsziele ausgewählt.

4. AKTIVE EINDRINGVERSUCHE Die ausgewählten Systeme werden aktiv angegriffen und etwaige Sicherheitslücken werden ausgenutzt.

5. ABSCHLUSSBERICHT Die gesammelten Ergebnisse werden in einem Abschlussbericht zusammengefasst. Der Bericht sollte auch eine Bewertung der gefundenen Schwachstellen vornehmen sowie Empfehlungen zur Beseitigung bzw. Behebung der Schwachstellen enthalten.

BEISPIELHAFTE VORGEHENSWEISE EINES PENETRATIONSTESTS

Aufgrund der Komplexität und Vielfalt von IT-Infrastrukturen und ihren Komponenten bieten sich auch vielfältige Gestaltungsmöglichkeiten von Penetrationstests. Viele Dienstleister bieten aus diesem Grund unterschiedliche Testmodule an, die flexibel nach Wunsch zusammengestellt werden können. Trotz aller Variabilität ist der grundlegende Ablauf eines Penetrationstests meist ähnlich und es gibt bestimmte Standardtestphasen, die in der Regel Bestandteile eines jeden Penetrationstests sind.

Im Downloadbereich finden Sie eine beispielhafte Beschreibung des methodischen Vorgehens bei der Analyse einer Webserviceschnittstelle.

> **DER KRIMINELLE HACKER WIRD DURCH DIE BEAUFTRAGUNG EINES PENETRATIONSTESTS MIT SEINEN EIGENEN MITTELN BEKÄMPFT, INDEM DER WHITE HAT-HACKER (PENETRATIONSTESTER) VERSUCHT, DIE GLEICHE PERSPEKTIVE EINZUNEHMEN UND „KRIMINELLE“ ENERGIE ZU INVESTIEREN, UM POTENZIELLE IT-SICHERHEITSLÜCKEN AUFZUSPÜREN.**

FAZIT

Ob IT-Infrastruktur, Webanwendungen oder eingesetzte Clients im Unternehmen – ein Penetrationstest überprüft, inwieweit die Sicherheit der IT-Systeme durch Bedrohungen von kriminellen Hackern gefährdet ist bzw. ob aktuelle Sicherheitsmaßnahmen greifen und ausreichend sind.

Die enge Kooperation mit dem Auftraggeber ist immens wichtig, weil sie dem „White Hat“ in puncto Informationen den entscheidenden Vorsprung und Vorteil bietet, den sich kriminelle Hacker meist erst mit teils erheblichem Aufwand erarbeiten müssen. So können IT-Schwachstellen behoben werden, bevor sie zum Sicherheitsvorfall führen. Oft ist es nur eine kleine, scheinbar unbedeutende Lücke, die immense wirtschaftliche Schäden oder Reputationsschäden verursacht. Es ist daher empfehlenswert, regelmäßige Penetrationstests fest in die IT-Arbeitsabläufe zu integrieren und das notwendige Budget dafür vorzuhalten.

Dieser Artikel ist mit freundlicher Unterstützung von Dr. André Markemann Technical Editing, PR der SySS GmbH entstanden, dem Marktführer für Penetrationstests.

STUDIE ZEIGT:

GESCHÄFTSFLÄCHEN WERDEN BESSER VOR EINBRÜCHEN GESCHÜTZT ALS DIE EIGENEN VIER WÄNDE

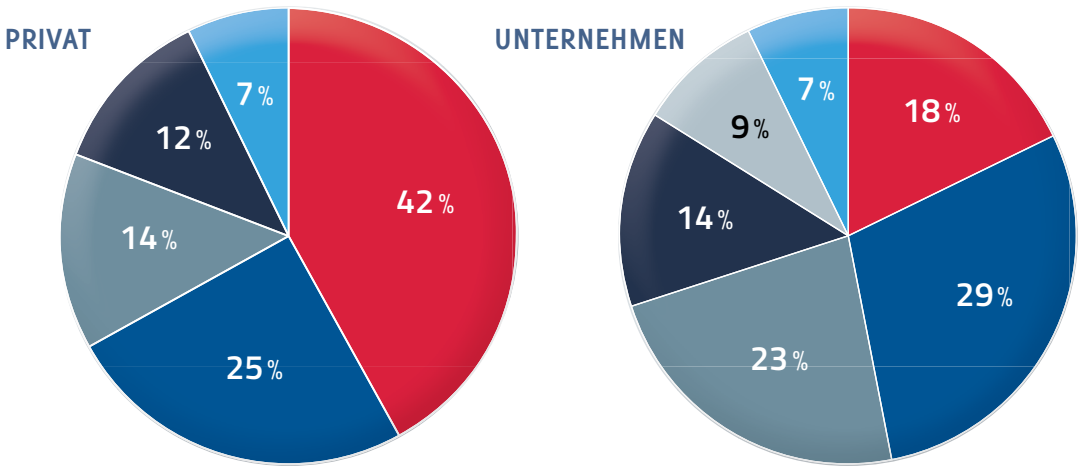
Einbrüche und somit das Eindringen in die Privatsphäre zählen zu den größten Ängsten der Deutschen. Beim Thema Einbruchschutz zeigt sich: Geschäftsflächen sind heutzutage mehr vor Einbrüchen und Überfällen geschützt als das eigene Zuhause. Das berichtet eine bundesweite repräsentative Studie zum Sicherheitsempfinden, die das Marktforschungsinstitut INNOFACT im Auftrag der Protection One GmbH durchgeführt hat.

Unternehmer schützen ihre Gewerbeflächen in höherem Maße und setzen in Sachen Sicherheit vermehrt auf Einbruchschutz. Trotz der verbreiteten Angst vor Einbrüchen zeigt die Studie, dass im Privatbereich hingegen relativ selten Sicherheitsvorkehrungen gegen Einbruch und Diebstahl getroffen werden. Dabei fokussiert sich die Online-Umfrage auf das Sicherheitsgefühl, also die Ängste der Menschen vor Einbrüchen und Überfällen sowie die damit verbundenen Sicherheitsvorkehrungen. Die empfundene Sicherheit beziehungsweise Unsicherheit sowie Maßnahmen zum Schutz von Hab und Gut werden dem Ist-Zustand der polizeilichen Kriminalstatistik gegenübergestellt. 1.584 Personen nahmen insgesamt an der Umfrage teil, davon 1.180 volljährige Privatpersonen und 404 Unternehmer, Selbstständige oder Geschäftsführer beider Geschlechter aus Gesamtdeutschland.

BERUFLICH VORSORGEN, PRIVAT SORGEN?

Gewerbeflächen werden im Allgemeinen besser geschützt als Privathaushalte. Dabei reagieren Privatpersonen der durchgeführten Studie zufolge weitaus emotionaler auf Einbrüche als Unternehmer. Mit 42 % fürchtet ein Großteil der befragten Privatpersonen psychische und emotionale Schäden bei Einbrüchen in den eigenen vier Wänden und eine Verletzung der Privatsphäre sowie des Sicherheitsgefühls. „Die Sorge, Opfer eines Einbruchs zu werden, steht in einem klaren Widerspruch zu den erbrachten oder geplanten Sicherheitsvorkehrungen der Deutschen“, resümiert Martin Smets, Unit Director der INNOFACT AG.

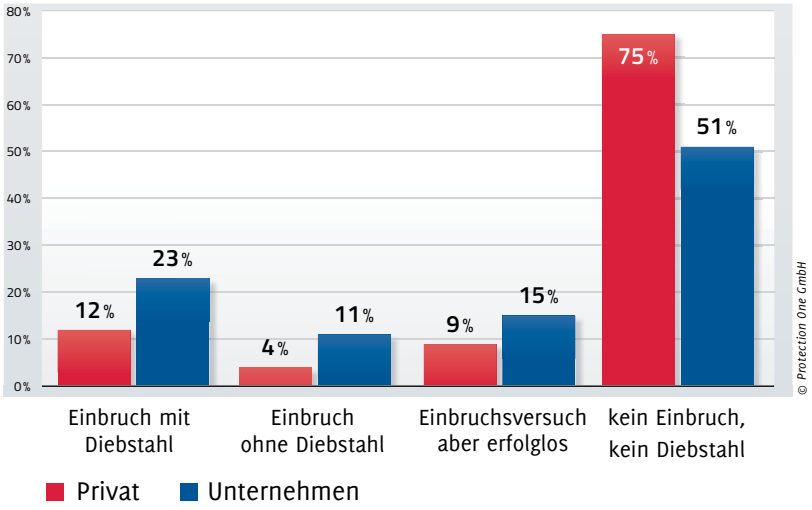
VOR WELCHEN SCHÄDEN UND FOLGEN EINES EINBRUCHS HABEN SIE AM MEISTEN ANGST?



Privatpersonen fürchten vor allem emotionale Schäden durch Einbrüche, Unternehmen hingegen Vandalismus und materielle Schäden.

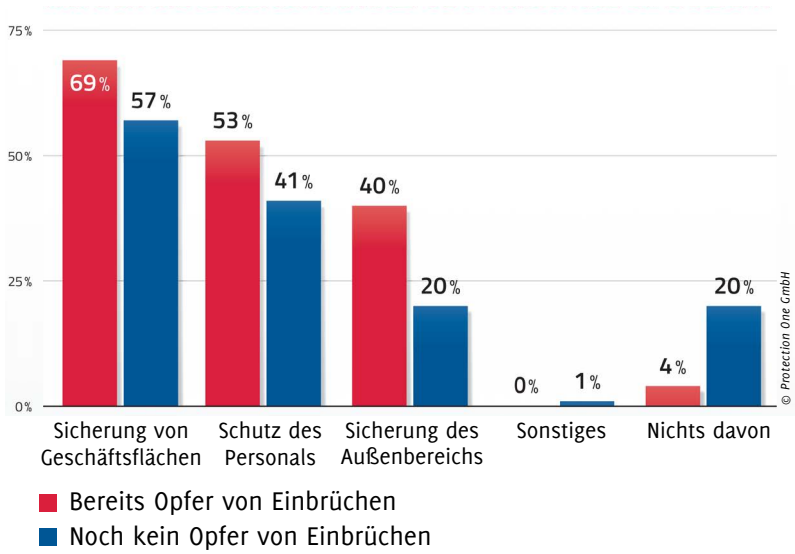
Für Unternehmer hingegen sind Emotionen im Rahmen von Einbruchdiebstählen mit 18 % weniger relevant. Sie sorgen sich häufiger um entstandene Schäden durch Vandalismus und Einbruch. Finanzielle Einbußen durch Neuanschaffungen fürchten 23 % der Unternehmer. Die Studie zeigt: Unternehmer setzen im Vergleich zu Privatpersonen deutlich mehr Sicherheitsvorkehrungen ein, um sich vor Einbrüchen zu schützen. Der Grund dafür erscheint simpel – die Einbruchsrate im Gewerbe verzeichnet eine höhere Opferzahl. Während 16 % aller befragten Privatpersonen angaben, bereits Opfer eines Einbruchs in den eigenen Privaträumen geworden zu sein, notiert das Gewerbe eine Opferzahl von 34 % aller befragten Unternehmer.

WAREN SIE SCHON OPFER VON ...?



Die befragten Unternehmen wurden deutlich häufiger Opfer von Einbrüchen und Diebstählen als die befragten Privatpersonen.

FÜR WELCHEN BEREICH IN IHREM GESCHÄFT/UNTERNEHMEN WÜRDEN SIE EINBRUCHS-/ÜBERFALLSCHUTZ EINSETZEN?



Unternehmen würden Einbruchs-/Überfallschutz eher aufrüsten als Privatpersonen.

AUS ERFAHRUNG SCHÜTZEN

Unternehmer schützen neben ihrem Personal (45 %) hauptsächlich ihre Geschäftsflächen (61 %). Dafür spielt vor allem die Tatsache, ob Unternehmer bereits negative Erfahrungen gemacht haben, eine große Rolle. Mit Blick auf die Zukunft wollen Unternehmer ihren Einbruchschutz an Gewerbeobjekten künftig mehr ausbauen, als Privatpersonen dies für ihre eigenen vier Wände vorhaben. Privatpersonen sind sich hingegen überwiegend einig: Aktiv werden sie erst dann, wenn etwas im eigenen oder nahen Umfeld passiert. So wollen sich 35 % der Privatpersonen erst dann über Sicherheitstechnik für ihr Zuhause informieren, wenn es Einbrüche oder Überfälle in der Nachbarschaft gegeben hat. 16 % würden bereits aufgrund von Polizeimeldungen und Statistiken über Sicherheitsvorkehrungen nachdenken.

VORSORGE VOR SORGE?

Wer erst dann aufrüstet, wenn es bereits zu spät ist, hat vor allem eines – den Schaden!

„VIELE DEUTSCHE SOLLTEN VORZEITIG IN RICHTUNG SICHERHEIT PLANEN, WENN DIE ANGST VOR EINBRÜCHEN UND DESSEN FOLGEN HEUTE SCHON VORHANDEN IST“, gibt Martin Smets zu bedenken.

Weitere Erkenntnisse über das Angstverhalten der Deutschen vor und nach einem Einbruch, alters- und geschlechterspezifische Einstellungen und Emotionen sowie typische Widersprüche zwischen Vorhaben und Handeln erfahren Sie auf folgender Webseite: **www.protectionone.de/webstudie-sicherheit/**

Protection One Alles sicher!

Dieser Artikel ist mit freundlicher Unterstützung der Protection One GmbH entstanden, die sich auf ganzheitlichen Einbruchschutz spezialisiert hat.

Sicher-Gebildet.de
Qualität bildet den Unterschied

E-LEARNING-TRAININGS HEALTH + SAFETY + SECURITY

AUSZUG AUS UNSEREM ANGEBOT

CORPORATE SECURITY:

- IT-Sicherheit
- Unternehmenssicherheit
- Compliance im Unternehmen
- Krisen- und Notfallmanagement
- Datenschutz und Datensicherheit
- Umgang mit Bombendrohungen & Co.
- Reisesicherheit bei Auslandsaufenthalten
- u. v. w.

HEALTH AND SAFETY:

- Arbeitssicherheit
- Erste-Hilfe Unterweisung
- Brandschutzunterweisung
- Wahrnehmung von Gefahren
- Richtiger Umgang mit Gefahrstoffen
- Gebäuderäumungsübung
- Räumungshelfer/-in
- u. v. w.

Besuchen Sie uns online unter www.Sicher-Gebildet.de

INTERVIEW MIT **JAN BERTHOLD, LEITER SICHERHEITSMANAGEMENT STIFTUNG HUMBOLDT FORUM IM BERLINER SCHLOSS**

ZUR PERSON:

Als studierter Sicherheitsmanager, Kriminologe, Polizeiwissenschaftler und zertifizierter Krisenmanager bewege ich mich nun seit fast 20 Jahren im Rahmen der privaten und öffentlichen Sicherheitsarchitektur. Dieser Weg führte mich über diverse operative Tätigkeiten, Ausschreibungsmanagement, Kundenberatung für Sicherheitsdienstleister, Beschaffung und Controlling entsprechender Services, der Implementierung und Koordination von Sicherheitsstrategien im Ausland hin zur sicherheitsstrategischen Gesamtverantwortung im Rahmen von Unternehmungen des Bundes, wie ganz aktuell der Leitung des Sicherheitsmanagements in der Stiftung Humboldt Forum im Berliner Schloss. Die Kernkompetenz des Humboldt Forums liegt in der inhaltlichen wie räumlichen Verflechtung von Kunst, Kultur, Natur, Wissenschaft, Forschung und Bildung.

SEHR GEEHRTER HERR BERTHOLD, VIELEN DANK, DASS SIE SICH DIE ZEIT NEHMEN, UNS ÜBER IHR INTERESSANTES TÄTIGKEITSFELD ZU BERICHTEN. STIFTUNG HUMBOLDT FORUM… WELCHE PLÄTZE, GEBÄUDE UND KULTURGÜTER FALLEN IN IHREN ZUSTÄNDIGKEITSBEREICH?

Als Leiter des Sicherheitsmanagements bin ich mit meinem Team für die Sicherheit aller Liegenschaften der Stiftung verantwortlich. Vorrangig ist dies das Humboldt Forum im Berliner Schloss sowie vier weitere Standorte. Im Bereich des Schutzes von im Humboldt Forum zukünftig auszustellender Exponate, arbeiten wir bereits jetzt eng mit den Kollegen und Kolleginnen der Staatlichen Museen zu Berlin, der Stiftung Stadtmuseum Berlin, Kulturprojekte Berlin sowie der Humboldt-Universität zu Berlin zusammen. Ziel unserer Arbeit ist es, die Sicherheit und Unversehrtheit beherbergter Kunst- und Ausstellungsobjekte, die unserer Gäste, der Mitarbeiter sowie den generellen Schutz der Infrastruktur unseres Hauses zu gewährleisten. Neben den hier ausgestellten Kulturgütern, die einen Großteil des Humboldt Forums für sich beanspruchen, verfügen wir zukünftig über einen hochfrequentierten Veranstaltungsbereich, über gastronomische Betriebe sowie Sonderausstellungsflächen, auf denen in Zukunft ganz unterschiedliche Projekte verwirklicht werden sollen.

Die konsequente Interdisziplinarität, die Internationalität und vor allem die Zugänglichkeit für alle, ohne augenscheinlich besonders restriktiv ausgerichtete Zugangsprozedere, bedingen dabei gleichzeitig einen besonders hohen Anspruch an unsere organisatorischen Standortsicherheitsmaßnahmen.

BEI DER ANZAHL AN EXPONATEN, EINER ZU ERWARTENDEN HOHEN VERANSTALTUNGS- UND DAMIT BESUCHERDICHTE SOWIE DER EINSTUFUNG DES BERLINER SENATES ALS BESONDERS SCHÜTZENWERTES OBJEKT STEHEN SIE SICHERLICH VIELERLEI THEMEN-, DELIKT-, UND PROBLEMFELDERN GEGENÜBER.

Das kann ich definitiv bejahen. Das Spektrum an Aufgaben, welche wir schon jetzt im Rahmen unserer strategischen Planung und taktischen Ausrichtung des Fachbereiches berücksichtigen müssen, ist enorm. Neben den eher „klassischen“ Schutzmaßnahmen, wie beispielsweise der Einzelobjektsicherung im Rahmen des Exponatenschutzes, stellt besonders die bereits erwähnte Zugänglichkeit des Humboldt Forums hohe Ansprüche an das Sicherheitsmanagement. Denn dort, wo viele Menschen aufeinandertreffen, in unserem Fall werden das schätzungsweise 3 bis 4 Millionen Besucher jährlich sein, sind sicherheitskritische Situationen nicht auszuschließen. Aufgrund der relativ schwer für Fremde zu identifizierenden Grundstücksgrenze des Humboldt Forums, rechnen wir mit entsprechenden Herausforderungen im Rahmen der Durchsetzung unserer Hausordnung.
Das Wegerecht der Öffentlichkeit in einigen Bereichen erfordert eine zusätzliche strategische Schwerpunktsetzung im Rahmen der Ausrichtung unserer Standortsicherheit sowie dem potenziellen Einsatz externer Sicherheitsdienste.

Unsere Abteilung plant und koordiniert zudem gemeinsam mit dem Senat, dem LKA und BKA Staatsbesuche, trifft ›››

Absprachen zum Umgang und zur Bekämpfung allgemeiner Kriminalität im Umfeld des Humboldt Forums und begleitet entsprechend planungsintensive, präventive Vorkehrungen.

WAS SEHEN SIE ALS HAUPTPROBLEM BEIM SCHUTZ ODER DER SICHERHEIT VON KULTURGÜTERN?

Nur wenige Wochen nach dem Kunstraub von Dresden ist dies recht einfach zu beantworten: Der Zwiespalt zwischen der Sicherung der Objekte und dem Zugang für die Öffentlichkeit. Herr Köhne, Präsident des Deutschen Museumsbundes, hat dies kürzlich recht gut formuliert: „Wir sind eben kein Banksafe“. Das trifft es ganz gut. Die Ausstellung der Exponate, welche nicht immer ausschließlich in verschließbaren, elektronisch gesicherten Vitrinen hinter Panzerglas stattfindet, sondern oft auch gewollt Besuchern und Besucherinnen greifbar nah auf Podesten sowie an Wänden präsentiert werden, setzt ein sehr durchdachtes Ineinandergreifen, eine effektive Verknüpfung von technischen, organisatorischen und vor allem auch personellen Maßnahmen voraus. Moderne Sicherungstechniken lassen auch in diesen Fällen Kompromisse zu, welche die vorgenannten Ausstellungsvarianten möglich machen. Spektakuläre Fälle wie die Diebstähle im Berliner Bode-Museum oder jüngst in Dresden zeigen allerdings, dass entsprechende Sicherungsmaßnahmen immer wieder angepasst, überarbeitet oder erweitert werden müssen. Hierbei besonders hervorzuheben die technische Redundanz entsprechender Sicherheitstechnik, welche auch potenzielle Manipulationen an der technischen Infrastruktur zuverlässig überbrücken muss. Eines unserer Hauptziele ist es, Tatanreize im Vorfeld zu entkräften.

IHRE TÄTIGKEIT UNTERSCHEIDET SICH JA SCHON WESENTLICH VON DER EINER KLASSISCHEN UNTERNEHMENSSICHERHEIT, BEI DER ES ZUM TEIL UM ANDERE SCHUTZZIELE GEHT. WIE SEHEN SIE DIE KÜNFTIGEN HERAUSFORDERUNGEN BEIM SCHUTZ VON KULTURGÜTERN – EGAL OB SCHLOSS, PARKANLAGE, KLEIN- ODER GROSSSTADT?

Wir hatten im Humboldt Forum das Glück, dass wir unsere fachlichen Ansprüche an ein effektives Sicherheitsmanagement von Anfang an mit in die Planungen einbringen konnten. Dabei ist es ein großer Vorteil, z. B. Sicherheitstechnik in der Bauphase grundlegend so platzieren und berücksichtigen zu können, dass spätere, meist aufwendige Nachrüstungen, Erweiterungen und damit verbundene Nachteile für den laufenden Betrieb reduziert werden. Wurde an dieser Stelle gut geplant, können künftige Erweiterungen zumeist zeit- und kostenschonend an die bereits bestehende Infrastruktur „andocken“, ohne essenziell in die vorhandene Bausubstanz eingreifen zu müssen. Dies ist gerade bei den großen, zumeist historisch gewachsenen Ausstellungshäusern, in zum Teil hunderte Jahre alten Gemäuern weitaus schwieriger. Eine große Herausforderung ist und bleibt definitiv der Spagat zwischen gelebter und gewollter Offenheit für alle interessierten Besucher und Besucherinnen bei gleichzeitiger Steigerung oder Aufrechterhaltung effizienter Standortsicherheitsmaßnahmen. Überall dort, wo technische bzw. bauliche Schutzmaßnahmen aus vorgenannten Gründen nicht gewollt oder umsetzbar sind, müssen prozessuale sowie organisatorische und damit auch personelle Maßnahmen greifen. Diese unterliegen vielen Einflussgrößen. Nicht alle Fehlerquellen können dabei immer hundertprozentig überblickt bzw. ausgeschlossen werden.

WAS ZIEHEN SIE FÜR SICH PERSÖNLICH ALS SCHLUSSFOLGERUNG AUS DIESER ANTWORT?

Stets auf dem „Laufenden“ zu bleiben. Neuen Sicherheitstechniken nicht immer bedingungslos zu trauen, dennoch immer offen für intelligente Systeme zu sein, welche vorgenannte Maßnahmen gut miteinander verbinden. Beispielsweise werden durch Neuerungen im Bereich der „künstlichen Intelligenz“ eine Vielzahl von

Bilder des Berliner Schlosses und des Foyer
Stiftung Humboldt Forum im Berliner Schloss (SHF) © SHF / Architekt: Franco Stella mit FS HUF PG

Möglichkeiten nutzbar, die so in der Vergangenheit nicht vorhanden waren. Hier bieten zum Beispiel moderne Videoüberwachungssysteme effektive, ressourcenschonende Möglichkeiten, datenschutzkonform Arbeitsschritte in der Detektion zu automatisieren und somit zum Teil proaktiv Schäden abzuwenden.

WELCHEN RAT KÖNNEN SIE ANDEREN PERSONEN, DEREN VERANTWORTUNG DIE STRATEGISCHE AUSRICHTUNG DER SICHERHEIT VON KULTURGÜTERN IST, MIT AUF DEN WEG GEBEN?

Grundsätzlich sehe ich mich nicht in der Position, schlaue Ratschläge zu erteilen. Eher möchte ich anregen, noch intensiver in den persönlichen und institutionellen Austausch zu treten. Jede Kulturstätte hat ihre ganz eigenen Herausforderungen, hat unterschiedliche Erfahrungen gemacht, eventuell Schadensereignisse durchlebt und kann somit im Rahmen eines „Best-Practice-Sharing“ anderen Häusern Ratschläge geben und berichten, welche jeweiligen Lösungsstrategien sich als besonders effektiv herausgestellt haben.

WIE WICHTIG IST DIE ZUSAMMENARBEIT MIT ÖFFENTLICHEN STELLEN UND WELCHE SEHEN SIE ALS PARTNER – FÜR EIN SICHERES MITEINANDER – AN IHRER SEITE?

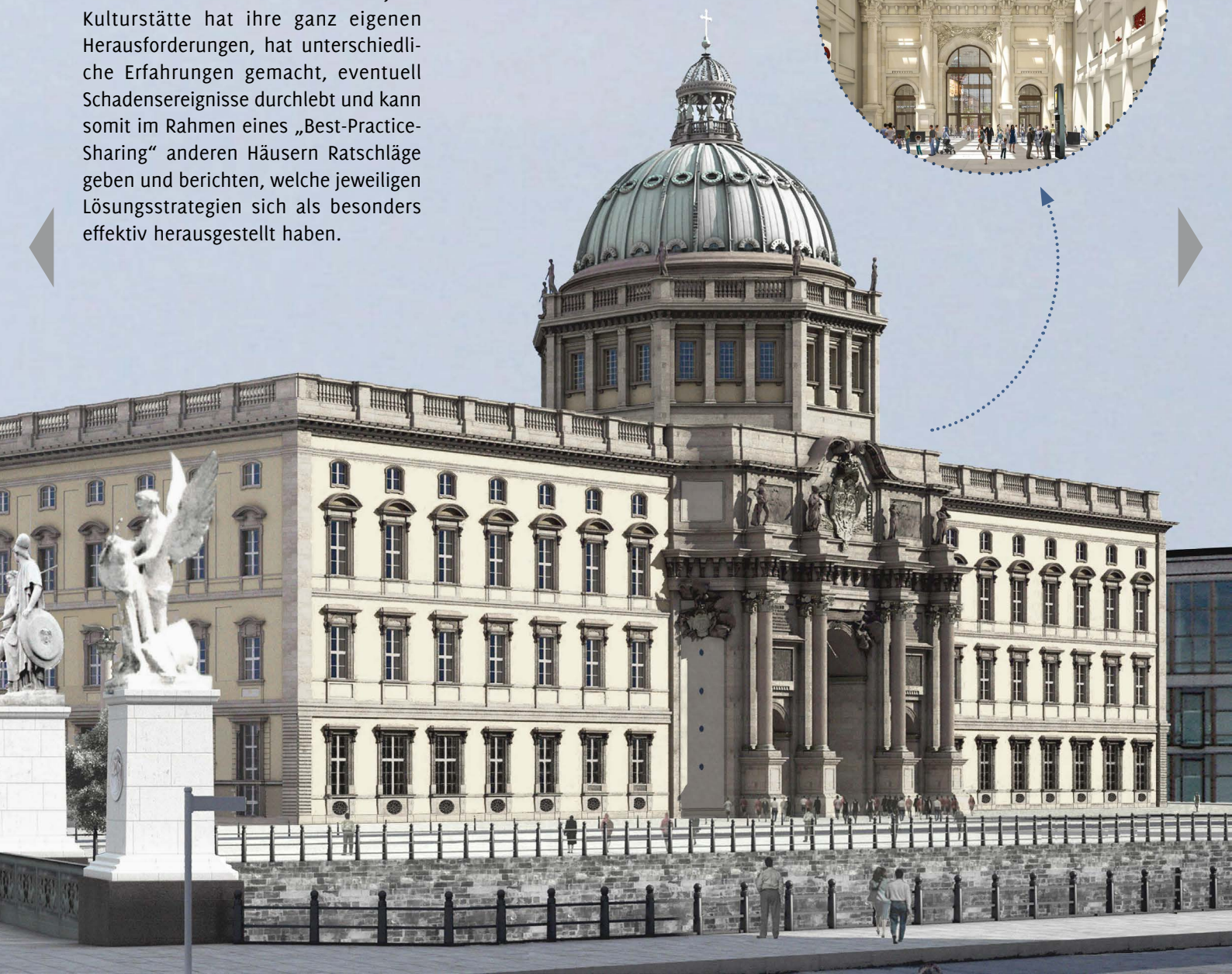
Bei einem so großen Bau- bzw. Kulturprojekt wie dem Humboldt Forum ist man von Anfang an mit vielen Institutionen im Austausch. Für uns im Sicherheitsmanagement primär relevant hierbei die Kollegen und Kolleginnen des Senats, der Berliner Polizei und der Feuerwehr. Selbstverständlich arbeiten wir darüber hinaus von Anfang an Schulter an Schulter mit den ausführenden Planer- und Fachfirmen beispielsweise aus den Bereichen der Gefahrenmelde- und Videoüberwachungstechnik zusammen.

ZU GUTER LETZT NOCH EINE FRAGE ZUR KÜNFTIGEN SICHERHEIT DES BERLINER SCHLOSS – KINDERSPIEL ODER HERAUSFORDERUNG?

Definitiv eine große Herausforderung.

VIELEN DANK, DASS SIE SICH DIE ZEIT FÜR EIN INTERVIEW GENOMMEN HABEN. VIELLEICHT LASSEN SIE UNS ZUR ERÖFFNUNG RÜCKWIRKEND AN IHREN PROJEKTERFAHRUNGEN TEILHABEN!

Sehr gerne.



In diesem Bereich stellen wir Ihnen nützliche Tools, Sicherheitsmessen sowie Behörden, Verbände und Institutionen mit Sicherheitsaufgaben vor. Zusätzlich finden Sie hier auch ausgewählte (Fach-)Bücher, die Ihnen die Welt der „Sicherheit“ noch anschaulicher vermitteln werden.

SICHERHEITSHINWEIS

DAS JAHR 2020 MACHT BETRUG LEICHT MÖGLICH

Neues Jahr, neue Zahl: doch diese Konstellation hat ihre Tücken.

Die Abkürzung der Jahreszahl beispielsweise neben Unterschriften auf Dokumenten, Verträgen oder Bestellungen kann leicht verändert werden. Wenn nur mit 01.03.20 unterschrieben wird, könnte ein Betrüger ohne große Umstände noch zwei Zahlen ergänzen.

So wird aus Ihrem potenziellen Neuvertrag ganz schnell ein Altvertrag aus dem Jahre 2007, 2013 oder 2019. Somit lassen sich Fristen und Garantien verkürzen oder verlängern oder gar Zahlungen und Gebühren rückwirkend fordern.

Da die Beweislast beim Geschädigten liegt, raten die Verbraucherzentralen dazu, Belege oder Kopien aufzuheben und vor allem das Jahresdatum ab sofort auszuschreiben.

01.10.2017
12.12.2019 07.06.2018

BUCHTIPP

ELEKTRONISCHE ZUTRITTSKONTROLLE

Ein Praxishandbuch für alle, die sich mit Zutrittskontrolle beschäftigen wollen oder müssen!
Der Einbau einer Zutrittskontrolle in Gebäude beschäftigt bundesweit nicht nur Sicherheitsmanager, Haustechniker oder technisch versierte und sicherheitserfahrene Personen, sondern auch Laien auf diesem Gebiet, die sich die Funktionalität einer Zutrittskontrolle sukzessive sehr mühsam erschließen müssen. Der „Aha-Effekt“ tritt dabei oft erst dann ein, wenn es zu spät ist. Und dies ist meist dann der Fall, wenn man bei der Errichtung feststellt, dass entscheidende Punkte nicht bedacht wurden.

Der Untertitel trifft es auf den Punkt. Das Handbuch von Marcus Lanz unterstützt bei der Planung und Einführung einer elektronischen Zutrittskontrolle in der Praxis, gibt wertvolle (Insider-)Tipps sowie verständliche technische Erklärungen und regt zu Fragen an, die im Vorfeld geklärt werden müssen und an die eher weniger im Vorfeld gedacht wird.

ZU DEN AUTOREN

Um Ihnen die gesamte Bandbreite der Sicherheit mit fundierten und praxisnahen Einblicken vermitteln zu können, verfolgen wir bei SICHERHEIT. Das Fachmagazin. das erfolgreiche Prinzip der Mehrautorenschaft. Wir arbeiten – passend zu den spezifischen Themen – ausschließlich mit fachlich versierten Experten mit jahrzehntelanger praktischer Berufserfahrung auf den jeweiligen Gebieten zusammen.

IMPRESSUM

SICHERHEIT. Das Fachmagazin. c/o SIUS Consulting® • Dorfaue 8b • 15738 Zeuthen
Telefon: +49 (0) 30 / 700 36 96 -5 • E-Mail: kontakt@sicherheit-das-fachmagazin.de • Geschäftsführer: Michael Blaumoser
Umsatzsteuer-ID: DE279558068 • ISSN: 2569-3816 • Erscheinungsweise: 4 x pro Jahr • Bildquelle: www.stock.adobe.com

SICHERHEIT.
DAS FACHMAGAZIN.
SICHERHEIT AUF DEN PUNKT GEBRACHT.