Das Magazin des
IT-Dienstleistungszentrums Berlin
06|22

#2

bITDZ & bytes

THEMENSCHWERPUNKT: IT-SICHERHEIT

Wir gegen Cyber-Kriminalität

I-KFZ: Datensicher auf dem Online-Amt

LEITSTELLE FÜR DIE CYBERABWEHR
Eröffnung des Security Operations Center

ITDZ BERLIN

dIT is drin:

Zentrale Cyberabwehr für die Berliner Verwaltung

Eröffnung des „Security Operations Center“ im ITDZ Berlin

Testen Sie Ihr Wissen!

IT-Sicherheits-Newbie oder IT-Sicherheits-Superbrain?

Wir gegen Cyber-Kriminalität

IT-Sicherheit für die Daten der Berliner Bürgerinnen und Bürger

Einer von uns

Im Gespräch mit Karsten Pirschel

Impressum // Herausgeber: IT Dienstleistungszentrum Berlin, Berliner Straße 112-115, 10713 Berlin, Telefon: 030/90222-0, E-Mail: post@itdz-berlin.de, Internet: www.itdz-berlin.de, **Konzept, Redaktion, Organisation:** IT-Dienstleistungszentrum Berlin, Unternehmenskommunikation, Angelika Schwenk (v.i.S.d.P.), Diana Dasch, Benjamin Ferchow, Katja Gärtner (Redaktionsleitung), Ela Özdemircelik, Sabine Schmuck, Anna Ulrike Susok, Nina Wüllner, E-Mail: redaktion@itdz-berlin.de; Lutz Leukhardt, die Textkolonie, **Grafikkonzept und Satz:** graphodata GmbH, **Druck/Auflage:** bITDZ & bytes wird im Druckzentrum des ITDZ Berlin unter Einhaltung der Green-IT-Richtlinien, auf Recyclingpapier gedruckt, Auflage: 2900 Exemplare. **Abonnement:** Wenn Sie bITDZ & bytes abonnieren oder abbestellen möchten, schreiben Sie bitte an die Redaktion: redaktion@itdz-berlin.de
Bildnachweis: Cover: ITDZ Berlin/Newpic; ITDZ Berlin/Newpic: S. 2, 4, 6, 10, 11, 12, 13, 18, 28; IDTZ Berlin/Petras: S. 3, 29, 30, 31; Seite 2: Adobe Stock/ipopba; Seite 3: Adobe Stock/Duminda; Seite 5: Adobe Stock/NicoElNino; Seite 14: Adobe Stock/Seventyfour; Seite 15: ITDZ Berlin; Seite 33: Adobe Stock/vegefox.com; U4: ITDZ Berlin/Deichblick

Liebe Leserinnen, liebe Leser,

als zentraler IT-Dienstleister des Landes verarbeitet und speichert das ITDZ Berlin die Daten von rund 3,7 Millionen Berliner Bürgerinnen und Bürger: Meldeinformationen, Steuerbescheide oder Polizeidaten werden über das Berliner Landesnetz übertragen und in unseren Rechenzentren sicher verwahrt. Der Schutz dieser sensiblen Daten vor Cyberangriffen, Hacking und Datenmanipulation gehört neben der Digitalisierung und Standardisierung der Verwaltungs-IT zu den Kernaufgaben des ITDZ Berlin. Denn eine sichere und widerstandsfähige IT ist das Fundament für moderne, digitale Verwaltungsservices – von der digitalen Akte bis zum digitalen Antrag, mit dem Sie bereits heute zahlreiche Anliegen schnell und bequem über das Internet erledigen können.

Darum legen wir in der aktuellen Ausgabe der bITDZ & bytes einen Schwerpunkt auf das Thema IT-Sicherheit. Wir berichten über die aktuellen Herausforderungen für die öffentliche Verwaltung, die nicht zuletzt durch den Krieg in der Ukraine deutlich zugenommen haben. Und wir zeigen ganz konkret, was das ITDZ Berlin unternimmt, um Cyberangriffe auf die zentrale IT des Landes Berlin zu erkennen und abzuwehren. So erhalten Sie Einblicke in unser Security Operations Center (SOC), das wir vor kurzem gemeinsam mit der Regierenden Bürgermeisterin von Berlin und dem Chief Digital Officer offiziell eröffnet haben.

Mit unserer Expertise und Erfahrung als BSI-zertifizierter IT-Dienstleister unterstützen wir unsere Kundinnen und Kunden der Berliner Verwaltung aber auch ganz direkt: Etwa bei der Vorbeugung und Bewältigung von IT-Sicherheitsvorfällen durch das Berlin-CERT (Computer Einsatz- und Reaktions-Team), mit Schwachstellentests und Sicherheitsscans sowie bei der Sicherheitsberatung im Rahmen der Einführung neuer Fachverfahren.

Es ist mir auch ganz persönlich eine Herzensangelegenheit, für das Thema IT-Sicherheit zu sensibilisieren. Denn nur so können wir die Digitalisierung der Verwaltung im wahrsten Sinne des Wortes sicher weiter voranbringen. Bürgerinnen und Bürger schenken uns ihr Vertrauen in einen verantwortungsvollen Umgang mit ihren persönlichen Daten. Das gilt es täglich unter Beweis zu stellen.

Ich wünsche Ihnen eine interessante und spannende Lektüre.

Ihr Marc Böttcher, Vorstand ITDZ Berlin

PortraIT

Schwerpunktthema:
Wir gegen Cyber-Kriminalität

Wir gegen Cyber-Kriminalität

IT-Sicherheit für die Daten der Berliner Bürgerinnen und Bürger

Die Arbeit der Verwaltung wird zunehmend digital: Die Meldedaten der 3,7 Millionen Berlinerinnen und Berliner werden online verarbeitet und in den Landesrechenzentren gespeichert. Gleichzeitig nimmt die Zahl der Cyberangriffe auch auf öffentliche Einrichtungen ständig zu. Die Profis für Berlins IT-Verteidigung arbeiten im ITDZ Berlin. Hier hat die IT-Sicherheit der Berliner Verwaltung höchste Priorität.

Deutschlands IT steht unter Druck. Allein im vorigen Jahr verzeichnete das Bundesamt für Sicherheit in der Informationstechnik (BSI) 14,8 Millionen Infektionen durch diverse Schadsoftware wie Viren, Trojaner oder Ransomware. 2021 haben sich diese Hackerangriffe schlicht verdoppelt. Derzeit entstehen etwa 400.000 neue Varianten von Schadprogrammen – pro Tag, wohlgemerkt. Diese Zahlen verdeutlichen, wie entscheidend heute hochprofessionelle Maßnahmen zur Gewährleistung der IT-Sicherheit sind. Denn sind Cyberangriffe erfolgreich, ist der Schaden, besonders für die IT der öffentlichen Verwaltung, groß: Erstmals musste im vergangenen Jahr der Landkreis Anhalt-Bitterfeld den Cyber-Katastrophenfall ausrufen, nachdem er Opfer eines Ransomware-Angriffs geworden war und die Angreifer in großem Umfang Daten verschlüsselt hatten.

Schauen wir auf Berlin: Was schätzen Sie, wie viele potentielle Angriffe es im Jahr 2021 pro Monat auf die zentrale IT-Infrastruktur des Landes Berlin gab? Eine vierstellige Zahl? Rund 300.000 Angriffe pro Monat? Tatsächlich wurden monatlich rund 1,2 Millionen unberechtigte Zugriffsversuche erkannt und abgewehrt. Eine Zahl, die verdeutlicht, wie wichtig der hochgradige Schutz von Daten, Netzen und Rechenzentren des Landes Berlin ist. Der Grund ist nicht trivial: All diese Anstrengungen bezeichnet man zwar als IT-Sicherheit oder IT-Security – doch genau genommen schützen sie die Menschen und deren hochsensible Daten, wie Melde- oder Steuerdaten vor Beeinträchtigungen, Manipulation und Datenmissbrauch. Eine wichtige Voraussetzung, um Vertrauen in die Nutzung neuer, digitaler Angebote der Verwaltung wie die Digitale Akte und den Digitalen Antrag zu schaffen. Deren Daten werden über das Berliner Landesnetz (BeLa), die Highspeed-Datenautobahn für die Datenkommunikation in der Hauptstadtverwaltung, übertragen und in den beiden großen Landesrechenzentren gespeichert. Verantwortlich für die IT-Sicherheit dieser zentralen IT-Infrastruktur ist das ITDZ Berlin.

„IT-Sicherheit ist mehr als je zuvor ein Thema, das die gesamte Gesellschaft betrifft.“, sagt Karsten Pirschel, IT-Sicherheitsbeauftragter im ITDZ Berlin. Er kontrolliert die Umsetzung und Einhaltung von Sicherheitsmaßnahmen (mehr zu Karsten Pirschel ➔ Seite 29).

„Jeder private Nutzer sollte sich mit den Grundlagen auseinandersetzen – und wir als IT-Dienstleister des Landes Berlin in aller Breite und der maximal möglichen Tiefe. Nur so können wir unserer Verantwortung für die Daten aller Berlinerinnen und Berliner gerecht werden.“

> „IT-Sicherheit ist mehr als je zuvor ein Thema, das die gesamte Gesellschaft betrifft.“

KARSTEN PIRSCHEL
IT-Sicherheitsbeauftragter im ITDZ Berlin

Schutz des Herzstücks

Das Herzstück der zentralen IT der Berliner Verwaltung bilden die beiden Landesrechenzentren, die das ITDZ Berlin betreibt. Sie sind nach den strengen Vorgaben des Bundesamtens für Sicherheit in der Informationstechnik zertifiziert. In den Rechenzentren werden die hochgradig sensiblen Daten wie Meldedaten, Daten des Finanzamts, Steuerinformationen, Polizeiakten von rund 3,7 Millionen Berlinerinnen und Berlinern und der Löwenanteil aller großen Fachverfahren der Berliner Landesverwaltung gespeichert. Rund 10.000 virtuelle Maschinen und über 1.000 physische Server besitzen eine Speicherkapazität von derzeit fünf PetaByte, also fünf Millionen Gigabytes. Das Hochsicherheitsrechenzentrum ist besonders umfangreich geschützt, sein Standort ist nur wenigen Menschen bekannt. Irgendwo in Berlin befindet es sich in einem unterirdischen Bunker mit 2.000 m² Fläche, drei Meter dicken Betonwänden, 2,5 Tonnen schweren Stahltüren, einem mehrstufigen Zugangskontrollsystem, einem ausgefeilten Brandschutz und Kühlungssystem sowie einer autarken Energieversorgung für den Ernstfall.

Bereits der rein physische Schutz der komplexen IT-Systeme und Daten der Berlinerinnen und Berliner ist also immens. Für deren Sicherheit im virtuellen Raum sorgen das Cyber Defence Center (CDC) und die Spezialisten des Computer Emergency Reponse Teams (CERT).

Berlins Cyber-Sicherheit im CDC

Ein Cyberangriff ist niemals laut und selten auffällig. Entsprechend geschärft muss die Analyse und Beobachtung der IT-Infrastruktur Berlins angelegt sein, um Angriffe zu erkennen und darauf adäquat zu reagieren. Das ist die Aufgabe des Cyber Defence Centers (CDC) Landesverwaltung. Die Security-Experten des CDC erkennen dank eines automatisierten 24/7-Monitorings Cyberangriffe auf Netze und Systeme und wehren sie ab. Dafür nutzen sie hochmoderne Security-Systeme und digitale Tools zur Cyberverteidigung, entwickeln präventive Schutzmaßnahmen, analysieren Anwendungen im forensischen Labor und testen das eigene System regelmäßig mit simulierten Attacken. Mitte April diesen Jahres wurde das neue „Security Operations Center“ (SOC) im ITDZ Berlin eröffnet – eine Leitstelle für die zentrale Cyberabwehr für die Berliner Verwaltung (Mehr dazu ➔ Seite 10).

CERT: Cyberprofis für den Ernstfall

Teil des CDC ist das Computer Emergency Response Team (CERT). Das CERT könnte man als präventive Cyber-Detektive und reaktive Eingreiftruppe bezeichnen. Denn diese hochspezialisierten Security-Expertinnen und -Experten unterstützen die Kundinnen und Kunden des ITDZ Berlins bei der Prüfung und Absicherung ihrer IT-Infrastruktur etwa durch spezielle Schwachstellenscans und bieten Schulungen im sicherheitsrelevanten Umgang mit Hard- und Software an. Registriert das CDC tatsächlich einen Angriff, analysiert das CERT sofort die Situation, sichert die Spuren und startet notwendige Gegenmaßnahmen.

Überwachung im eigenen Netz

Das Land Berlin besitzt ein eigenes, komplett autarkes IT-Netz – das Berliner Landesnetz (BeLa). Es ist heute das größte deutsche Verwaltungsstadtnetz für Hochgeschwindigkeitskommunikation. Über dieses Netz erfolgt der zentrale Austausch von Sprach- und Datenkommunikation in der Berliner Verwaltung. Auch das BeLa ist nach BSI-Richtlinien zertifiziert, wird durch das Security Operations Center (SOC) ständig überwacht und seine Sicherheit durch 40 Mitarbeitende begleitet.

ISMS: Sicherheit mit System

ISMS ist die Abkürzung für Informationssicherheitsmanagementsystem. So lang der Begriff ist, so umfangreich ist auch das System dahinter. Es handelt sich um ein datenbankgestütztes Tool, das die kaufmännischen Abläufe nach BSI-Vorgaben analysiert, weiterentwickelt und zertifiziert. Dazu zählen beispielsweise Bereiche wie das Personalmanagement, die Sicherung von Daten, die Vermittlung von Security-Wissen und die Vorbereitung auf Sicherheitsszenarien.

Zertifizierte IT-Sicherheit

Das ITDZ Berlin ist seit 2015 als bundesweit erster IT-Dienstleister mit dem ISO 27001 Zertifikat des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ausgezeichnet. In Deutschland definiert das BSI hohe, strenge und klare Vorgaben, wie der sogenannte IT-Grundschutz in Verwaltung und Unternehmen gestaltet sein muss. Die BSI-Standards definieren dabei Methoden und Prozessen, wie IT-Verantwortliche die Informationssicherheit umzusetzen haben – vom Schutz der Daten, Hard- und Software bis zur Einrichtung des Informationssicherheits-Managementsystems. Entsprechend gelten diese Vorgaben auch für das Berliner Landesnetz, die Rechenzentren sowie alle Prozesse im ITDZ Berlin. Wo also BSI draufsteht, ist hohe IT-Sicherheit drin.

Mitglied in einer starken Allianz

Gemeinsam sind wir stärker. Aus diesem Grund ist das ITDZ Berlin aktives Mitglied in der Allianz für Cyber-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik. Rund 1.200 Unternehmen und Institutionen tauschen sich hier zu neuen Sicherheitsrisiken und Maßnahmen aus und beschließen Kooperationen, um die Widerstandsfähigkeit des Standortes Deutschland gegen Cyberangriffe zu erhöhen.

Kommt das Jahrhundert der Cyber-Angriffe?

Und wie geht es weiter bei der IT-Sicherheit für das Land Berlin? Eines steht bereits jetzt fest: Zahl und Qualität der Angriffe steigen weiter. So erfasst der aktuelle „Lagebericht Cybercrime 2021“ des Bundeskriminalamts eine Steigerung der Cyberstraftaten um 12 Prozent gegenüber dem letzten Jahr. Damit wachsen auch die Anforderungen an notwendige Maßnahmen sowie die Komplexität zur Betreuung aller Sicherheitssysteme. Eine Aufgabe, auf die das ITDZ Berlin für die Hauptstadt vorbereitet ist – für eine maximal mögliche IT-Sicherheit in der Verwaltung und den Schutz sensibler Daten nach den höchsten Standards.

Die 7 Tätermotive bei Cyberattacken

1 **Staatliche Spionage:** Cyberangriffe sind heute immanenter Teil von Konflikten zwischen Staaten. Sie versuchen, kritische Infrastrukturen lahmzulegen oder die Kommunikation und Daten von Staatsorganen zu kompromittieren. Diese Angriffe sind außerordentlich mächtig und professionell, da sie mit einem hohen staatlichen Budget finanziert werden.

2 **Private Erpressung:** Wer die Daten einer Person besitzt, hat gegen diese Person ein veritables Druckmittel in der Hand – entweder um sie zu bestimmten Handlungen zu zwingen oder die Daten im Namen des Inhabers zu missbrauchen.

3 **Finanzielle Forderungen:** Daten sind wertvoll – werden sie gekapert, verlangen Hacker häufig finanzielle Transaktionen. Werden die Zahlungen geleistet, stellt sich häufig heraus, dass die Daten bereits zerstört sind.

4 **Zerstörung:** Die reine Lust an der Zerstörung und Lahmlegung von Systemen ist für manche Hacker ebenfalls ein Antrieb. Sie betreiben sozusagen virtuellen Vandalismus.

5 **Wirtschaftsspionage:** Für Kundinnen und Kunden des ITDZ Berlin weniger relevant, dennoch ein hoher Motivationsfaktor für Täter: Die Kaperung von Unternehmensdaten, um einem Auftraggeber einen Wettbewerbsvorteil zu verschaffen oder Zugriff auf Neuentwicklungen und Knowhow zu erhalten.

6 **Geltungsdrang:** Manche Hacker sind schlicht eitel. Sie attackieren ein System ausschließlich, um darin ein kleines „Mitbringsel“ zu hinterlassen und zu zeigen: Ich war bei euch drin, ich habe es geknackt (ein sog. Website-Defacement).

7 **Persönliche Gründe:** Gelegentlich führen persönliche Gründe eines Hackers oder eines Auftraggebers zu einem Angriff. Rache, Eifersucht oder Neid können Grund genug sein für eine Attacke auf einen Rechner oder Server.

ERÖFFNUNG DES
„SECURITY OPERATIONS CENTER“ IM ITDZ BERLIN

Zentrale Cyberabwehr für die Berliner Verwaltung

Cyberbedrohungen durch Hackerangriffe, Schadprogramme und Sicherheitslücken haben in den letzten Jahren stark zugenommen. Angriffsziele sind zunehmend die persönlichen Daten von Bürgerinnen und Bürgern. Das ITDZ Berlin verarbeitet innerhalb seiner Netze und Rechenzentren die Daten von 3,7 Millionen Berlinerinnen und Berlinern. Zum verstärkten Schutz dieser sensiblen Daten vor Cyberbedrohungen eröffneten die Regierende Bürgermeisterin von Berlin, Franziska Giffey, und ITDZ-Vorstand Marc Böttcher gemeinsam mit Dr. Ralf Kleindiek, Staatssekretär für Digitales und Verwaltungsmodernisierung und Chief Digital Officer des Landes Berlin, am 13. April 2022 das neue „Security Operations Center (SOC)“ im ITDZ Berlin.

Dr. Ralf Kleindiek, Franziska Giffey, Marc Böttcher und Anne Lolas (stellvertretende Vorständin ITDZ Berlin) im neuen Security Operations Center. Vom modernen Leitstand aus erfolgt rund um die Uhr die Erkennung und Abwehr von Angriffen auf die zentrale IKT-Infrastruktur des Landes Berlin.

3, 2, 1 – Der rote Knopf startete die 10 m² große Monitorwand des Security Operations Centers. Sie zeigt auf einen Blick und in Echtzeit Statistiken, Daten und Schwellenwerte der automatisierten 24/7-Systemüberwachung.

„IT-Sicherheit muss aktiv gemanaged, kontinuierlich angepasst und professionell umgesetzt werden.“

MARC BÖTTCHER
Vorstand des ITDZ Berlin

Franziska Giffey: „Mit dem Security Operations Center gehen wir einen weiteren Schritt zum Schutz der IT-Infrastruktur des Landes und für die Berlinerinnen und Berliner.“

Dr. Ralf Kleindiek, Franziska Giffey, Anne Lolas und Marc Böttcher
auf dem Weg zur Pressekonferenz im ITDZ Berlin

So viel ist sicher

Im Security Operations Center erfassen und analysieren die Expertinnen und Experten des ITDZ Berlin täglich rund ein Terabyte (1.000 Gigabyte) Daten aus verschiedenen IT-Systemen wie Firewalls, Routern, Servern und Netzwerkkomponenten zentral und bewerten diese nach ihrer Kritikalität. Im Falle eines Cyberangriffs erfolgt die Alarmierung nach einem BSI-zertifizierten, festgelegten Alarmierungsprozess und in enger Abstimmung mit dem Landesbevollmächtigten für Informationssicherheit. Nach Einleitung von Sofortmaßnahmen informiert das Berliner Computer Emergency Response Team (CERT) ggf. betroffene Behörden und empfiehlt entsprechende Maßnahmen zum Schutz oder zur Gefahrenabwehr.

„Die Berlinerinnen und Berliner müssen darauf vertrauen können, dass ihre persönlichen Daten, die sie mit öffentlichen Einrichtungen teilen, sicher sind“, sagte die Regierende Bürgermeisterin Franziska Giffey. „Bedrohungen durch Cyberangriffe sind reale Gefahren für die Demokratie, insbesondere in der aktuellen Situation. Der Krieg in der Ukraine wird nicht nur mit Waffen geführt, sondern auch im Netz, weit über die Grenzen des Landes hinaus. Mit dem Security Operations Center gehen wir einen weiteren Schritt zum Schutz der IT-Infrastruktur des Landes und für die Berlinerinnen und Berliner.“

IT-Sicherheit ist keine Nebensache, sondern muss Standard werden

Im neuen „Security Operations Center (SOC)“, einem modernen Leitstand, erfolgt rund um die Uhr die Erkennung und Abwehr von Cyber-Angriffen auf das Berliner Landesnetz und die Landesrechenzentren. Security-Expertise und moderne Verfahren zur Cyberabwehr werden hier gebündelt und Erkenntnisse zur IT-Sicherheit aus einem Echtzeit-Lagebild für alle Berliner Behörden aufbereitet und durch das ITDZ Berlin zur Verfügung gestellt.

Marc Böttcher, Vorstand des ITDZ Berlin: „Gefahren durch Hackerangriffe, Schadprogramme und Sicherheitslücken nehmen seit Jahren zu. Unsere Erfahrung zeigt, dass IT-Sicherheit aktiv gemanaged, kontinuierlich angepasst und professionell umgesetzt werden muss. Im SOC bündeln wir Expertise, modernste Technik und Organisation. So wird es möglich, auch das Thema IT-Sicherheit für die Behörden und Einrichtungen der Berliner Verwaltung auf einem hohen Niveau zu standardisieren.“

„Informations- und IT-Sicherheit sind Grundvoraussetzungen für die Digitalisierung der Verwaltung und Online-Services wie den Digitalen Antrag und die Digitale Akte“, sagt Dr. Ralf Kleindiek, Staatssekretär für Digitales und Verwaltungsmodernisierung und Chief Digital Officer des Landes Berlin. „Mit dem Security Operations Center im ITDZ Berlin stärken wir die IKT-Sicherheitsstruktur des Landes Berlin mit modernen Methoden zur Cyberabwehr, hochqualifiziertem Fachpersonal und einem zentralen, wirtschaftlichen Betrieb. So unterstützen wir sowohl die Verwaltung als auch die Berlinerinnen und Berliner aktiv für die Umsetzung und Nutzung eines sicheren, digitalen Bürgerservice“.

Das neue Security Operations Center im Blitzlichtgewitter. Rund 40 Journalistinnen und Journalisten informierten sich vor Ort über Methoden und Maßnahmen zur Cyberabwehr.

Aus erster Hand: **Franziska Giffey** im Gespräch mit den IT-Security-Operatoren des ITDZ Berlin.

Frank Schreiber, langjähriger Empfangsmitarbeiter des ITDZ Berlin, freute sich über die persönliche Begrüßung der Regierenden Bürgermeisterin

Dr. Tim Freyer (links), Abteilungsleiter Kommunikationsdienste, und **Olaf Hoßfeld**, Fachbereichsleitung Cyber Defence Center Landesverwaltung. Die beiden ITDZ Berlin-Experten standen Rede & Antwort.

Für weitere Einblicke: Unser Video zur SOC-Eröffnung.

Im Fokus: die 10 m2 große Monitorwand.

„Mit dem Security Operations Center im ITDZ Berlin stärken wir die IKT-Sicherheitsstruktur des Landes Berlin mit modernen Methoden zur Cyberabwehr.“

DR. RALF KLEINDIEK
Staatssekretär für Digitales und Verwaltungsmodernisierung und Chief Digital Officer des Landes Berlin

Cybersicherheit in Zahlen

Leistungen des Security Operations Centers

analysierte Datenmenge
rund **1 Terabyte** **(1.000 Gigabyte)** pro Tag

Zahl abgewiesener Zugriffe (potentielle Angriffe)
rund **1,2 Millionen** pro Monat

erkannte Spam-Mails
über **530.000** pro Monat

erkannte Viren in E-Mails
rund **3.000** pro Monat

BenefIT

Wo IT-Standards Erfolgsgeschichte schreiben

DIGITAL UND SICHER

Seine Agenda: Berlins Verwaltung

Klaus-Peter Waniek ist Landesbevollmächtigter für Informationssicherheit der Berliner Verwaltung - ein langer Titel für eine Aufgabe, die oft kurze Dienstwege für schnelle, abgestimmte Entscheidungen braucht. Im Gespräch gibt der Experte für Informationssicherheit einen Einblick in seine Arbeit.

Herr Waniek, wie kann man sich Ihre Arbeit als Landesbevollmächtigter für Informationssicherheit vorstellen?
Im Land Berlin setzt das Gesetz zur Förderung des E-Governments - kurz E-Government-Gesetz Berlin - die Rahmenbedingungen für die Digitalisierung der Berliner Verwaltung. Darin ist auch festgehalten, welche Aufgaben im Bereich Informationssicherheit umzusetzen sind und damit in meiner Verantwortung liegen.

Können Sie das genauer erklären?
Informationssicherheit unterliegt ständigen Veränderungen. Es ist ein Prozess und kein Zustand. Die zentrale IKT-Sicherheitsarchitektur ebenso wie die Standards für die IKT-Sicherheit im Land Berlin müssen ständig weiterentwickelt werden. Dabei ist es ist wichtig, die Umsetzung der passenden Maßnahmen zu steuern, zu überwachen und immer weiterzudenken. Mit dem Verständnis, dass Informationssicherheit bei allen und nicht nur digitalen Verwaltungsprozessen umzusetzen ist, haben Sie meine Jobbeschreibung.

Wie sehr sind Sie dabei operativ für die IT-Security des Landes Berlin tätig?
Natürlich nicht bei der tatsächlichen Cyber-Abwehr, denn dafür gibt es ja die Spezialisten im ITDZ Berlin wie beispielsweise im CERT oder dem Cyber Defence Center Landesverwaltung. Bei mir liegt die operative Steuerung all jener Prozesse, die behördenübergreifend die Informationssicherheit in den Behörden und Einrichtungen der Verwaltung sichern und erhöhen. Ich sehe meine Rolle in einer Art fachlicher Management-Funktion in Zusammenarbeit mit dem ITDZ Berlin sowie mit den Informationssicherheitsbeauftragten in der Verwaltung. Gemeinsam definieren wir die Weiterentwicklung der Informationssicherheit gemäß den sich ändernden Anforderungen, setzen sie um und berichten regelmäßig über den Umsetzungsstand.

Klaus-Peter Waniek
Landesbevollmächtigter für Informationssicherheit

„Informationssicherheit ist ein Prozess und kein Zustand.“

Die Begriffe „Informationssicherheit“ und „IT-Sicherheit“ werden gerne vermischt oder verwechselt. Deshalb jetzt einmal mit den Worten eines Profis: Worin liegt der Unterschied?

Begriffe wie Informationssicherheit, Cybersicherheit oder Digitale Sicherheit werden oft beliebig, auch mit Bezug auf die Verwaltung verwendet, weil sie sich in ihren Inhalten durchaus überlagern. Begonnen hat es mal mit dem Begriff „IT-Sicherheit“, der sich rein auf den Technikeinsatz bezieht. Aber schnell wurde klar, dass es nicht allein um die Sicherheit der Informationstechnik geht. Die „Informationssicherheit“, also Sicherheit der Informationen einer Organisation in jeglicher Form - digital, auf Papier und auch das Wissen der beteiligten Menschen betreffend - ist zu gewährleisten.

Informationssicherheit in der Verwaltung beinhaltet neben sicheren Prozessen mit oder ohne IT-Unterstützung auch die Sicht auf die handelnden Menschen. Damit werden auch Anforderungen anderer Schutzbereiche wie dem Datenschutz maßgeblich unterstützt.

Worin bestehen die größten Herausforderungen?

Maßnahmen gegen Risiken in der Informationssicherheit regulieren das Handeln und können deshalb als unbequem und Komfort einschränkend wahrgenommen werden. Heute werden häufig gleich mehrere Passwörter für unterschiedliche Anwendungen am Arbeitsplatz benötigt, die auch noch alle sicher und komplex sein sollen. Letztlich ist eine große Herausforderung für Informationssicherheit in der Verwaltung, Akzeptanz für die darauf optimierten Verwaltungsabläufe zu erreichen. Dazu zählt jedes Verhalten, vom Umgang mit USB-Sticks bis hin zum Einsatz „privater“ Lösungen, um die Arbeit zu „unterstützen“.

So gesehen steht wie so oft der Mensch im Mittelpunkt der Informationssicherheit.

Ein Weg, ein höheres Niveau an IT-Sicherheit zu erreichen, ist die Standardisierung von Hardware und Software in Ämtern und Behörden. Können Sie erklären, weshalb das so ist?

In der Berliner Verwaltung sind tausende Rechner mit aktuell noch unterschiedlichsten Hard- und Softwarelösungen im Einsatz. Das heißt wiederum, alle bei laufendem Betrieb auf dem aktuellen Stand zu halten, ohne dass die Aktualisierung selbst zum störenden Faktor wird. Das bedeutet, dass pro Rechner der Aufwand für die bestmögliche IT-Sicherheit enorm ist und sich teilweise trotz aufwendiger Pflege rein zeitlich Sicherheitslücken auftun bis die Aktualisierung erfolgt ist. Auf gut Deutsch ist das ein Schreckensszenario für jeden IT-Security-Profi.

Und eine Standardisierung der IT ist hier die Lösung?

Ja. Denn wären sowohl die Rechner als auch die Anwendungen darauf weitgehend mit einheitlicher Software ausgestattet sowie mit gleicher und aktueller Versionierung in Benutzung, könnten die Patches zur Aktualisierung viel schneller, zentral gesteuert umgesetzt werden. Damit wären alle Arbeitsplätze gleichermaßen schnell und einheitlich vor Angriffen geschützt. Dort sind wir noch nicht, aber dort möchten wir hin. Nein, ich korrigiere mich: Dort *müssen* wir hin.

Wie genau sieht dabei Ihre Zusammenarbeit mit dem ITDZ Berlin aus?

Mit dem ITDZ gibt es zahlreiche Aspekte der Zusammenarbeit, beginnend bei der Umsetzung der IKT-Architektur, dem BerlinPC und den IKT-Basisdiensten. Natürlich erbringt das ITDZ Berlin auch konkrete Leistungen zur Gewährleistung der IKT-Sicherheit. Das umfasst etwa das Berlin-CERT, das Cyber Defence Center Landesverwaltung und auch die BSI-Zertifizierung des ITDZ.

In verschiedenen Formaten für den fachlichen Austausch diskutieren wir aktuelle Sicherheitsereignisse, besprechen die erforderliche Reaktion darauf, stimmen unser Vorgehen ab und etablieren diverse Tools, um unsere Arbeit möglichst optimal zu koordinieren.

Was bedeutet Ihnen persönlich diese Zusammenarbeit?

Der fachliche Austausch ist für uns alle sehr wichtig. Wir geben einander Wissen weiter und unterstützen uns bei anstehenden Themen und Aufgaben. So können wir besonders schnell eine spezielle Expertise abrufen und entsprechend schnell und professionell handeln. Und Sie können sich ja vorstellen: Angesichts der unheimlichen Dynamik rund um die Informationssicherheit werden uns in absehbarere Zeit die spannenden Themen nicht ausgehen.

NEUER STANDARD
FÜR MEHR SICHERHEIT

Der BerlinPC

„Für uns ist wichtig, dass wir sensible Daten schützen und gleichzeitig eine hohe Verfügbarkeit sicherstellen.“

RÜDIGER SNIEHOTTA
Leiter des Fachbereichs
„Desktopbetrieb BerlinPC“ im ITDZ Berlin.

Arabische Zahlen, lateinische Buchstaben oder das metrische System – sie alle sind selbstverständliche Wegbegleiter unseres Alltags. Aber wie sähe unser Leben wohl ohne diese Standards aus? Vereinheitlichungen helfen uns dabei, uns auszutauschen, zu kommunizieren und zu interagieren – kurz: sie vereinfachen unser Leben. Mit der Digitalisierung der Verwaltung verfolgt das Land Berlin dieses Ziel auch für den Austausch zwischen den Behörden und ihren Schnittstellen zu den Bürgerinnen und Bürgern.

BerlinPC

Eine zentrale Rolle spielt dabei die einheitliche Arbeitsplatz-Ausstattung der Mitarbeitenden in den Berliner Behörden. Um diese zu erreichen, wird es zukünftig einen einheitlichen IKT-Arbeitsplatz mit seinem Herzstück, dem standardisierten BerlinPC geben.

Die Neuerung gegenüber bisherigen Komponenten besteht vor allem darin, dass der BerlinPC als zentraler, im Rechenzentrum des ITDZ Berlin verorteter, Desktop betrieben wird – ein Desktop as a Service (DaaS). Damit erhalten zwar alle Mitarbeitenden ein festes Endgerät (die Rechner gibt es in verschiedenen Ausführungen, bspw. als Desktop-PC oder als Laptop). Das Gerät ist aber jederzeit austauschbar, da die wesentlichen Arbeitsschritte nicht auf dem Rechner, sondern im Rechenzentrum des ITDZ Berlin erfolgen. Der kommende Landesstandard, BerlinPC, ist neben allen technischen Features vor allem auf ein Kriterium ausgerichtet: IT-Sicherheit. Ein wichtiger Vorteil liegt in diesem Zusammenhang in der Zentralisierung des Systems. Dadurch können Sicherheits-Updates und Softwareaktualisierungen zentral und zeitnah eingespielt werden und sind sofort für alle Nutzenden verfügbar. Außerdem laufen auf den zentralen Systemen im Rechenzentrum des ITDZ Berlin verschiedene Schutz- und Antiviren-Anwendungen, die damit ebenfalls alle Nutzenden abdecken.

Um darüber hinaus zu verhindern, dass Viren, Trojaner oder andere Schadsoftware über den BerlinPC eindringen können, lag ein besonderes Augenmerk auf der Verbindung zum Internet. Dazu wird der BerlinPC mit zwei verschiedenen Browsern geliefert. Der eine stellt eine Verbindung zum Internet her, der andere eine zum Berliner Landesnetz. Der Internet-Browser liegt dabei im Rechenzentrum des ITDZ Berlin in einer besonders isolierten Umgebung, sodass eine Kompromittierung nur diesen Bereich betreffen würde – andere Systeme bleiben geschützt.

Der BerlinPC ist ein wichtiger Baustein für die Digitalisierung der Verwaltung und hilft, Abläufe zu standardisieren. Zentral ist und bleibt dabei der Schutz der Daten der Berlinerinnen und Berliner.

„Für uns ist wichtig, dass wir ein Kompromittieren unserer Systeme verhindern, sensible Daten schützen und gleichzeitig eine hohe Verfügbarkeit sicherstellen“, sagt Rüdiger Sniehotta, Leiter des Fachbereichs „Desktopbetrieb BerlinPC“ im ITDZ Berlin.

AudIT

IT-Sicherheit im Fokus

KOMFORTABEL UND VERLÄSSLICH

Datensicher auf dem Online-Amt

Die Zahl der Online-Verfahren für Bürgerinnen und Bürger wächst. Das ITDZ Berlin stellt dabei sicher, dass die Verwaltungen die Anforderungen an die IT-Sicherheit erfüllen. Ein Beispiel ist i-Kfz. Seit Herbst 2019 lässt sich ein Großteil der Prozesse rund um das eigene Fahrzeug online erledigen. Komfortabel, verlässlich und mit Unterstützung des ITDZ Berlin hochgradig datensicher.

Lange Wartezeiten bei der Kfz-Zulassungsstelle? Das ist Vergangenheit. Denn seit dem 1. Oktober 2019 bietet das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) die Online-Zulassung und damit eine vollständig internetbasierte Fahrzeugzulassung an. Das Fachverfahren ist Teil der nationalen E-Government-Strategie, die 2010 beschlossen wurde. Technisch basiert dieses Angebot auf der i-Kfz-Lösung der ekom21, einem der größten Hersteller im Zulassungswesen. „Es gibt per se nicht viele Anbieter in diesem Bereich“, erklärt Philipp Kownatka von der Kfz-Zulassungsbehörde Berlin. „Die ekom21 erfüllte die technischen Vorschriften und betrieblichen Regeln des Landes Berlin sowie die Mindestsicherheitsanforderungen des Kraftfahrt-Bundesamts, um ein Portal zu betreiben.“ Dazu zählen beispielsweise Audits und Penetrationstests, für die die jeweiligen Zulassungsbehörden verantwortlich sind.

Es brauchte einen IT-Partner - diese Aufgabe übernahm das ITDZ Berlin.

Standardisierung trifft Sicherheit

Ziel des LABO war es, eine standardisierte Software zu nutzen statt eine eigene Lösung entwickeln zu lassen. Denn Standards sind bewährt, durchdacht, mehrfach getestet und erfüllen „die Basics“ in Sachen Sicherheit, wie es Philipp Kownatka nennt. Dazu zählen nach Vorgaben des Kraftfahrt-Bundesamts Vorgaben zur Technik, zur Informationssicherheit sowie verfahrensspezifische Anforderungen (mehr dazu ➔ Infobox). „Die Erfüllung solcher Sicherheitsstandards ist sinnvoll und notwendig, da die Fachverfahren mit sensiblen Daten der Bürgerinnen und Bürger arbeiten“, ergänzt Kownatka. Im Falle von i-Kfz sind das persönliche Daten wie Name und Anschrift, aber auch Kfz-bezogene Daten wie verdeckte Sicherheitscodes auf Stempelplaketten der Kennzeichen, Sicherheitscodes der Zulassungsbescheinigung Teil I, die Fahrzeug-Identifizierungsnummer, die Nummer der elektronischen Versicherungsbestätigung sowie Informationen zur Bezahlung entweder via ePayment-System oder über eine persönliche IBAN-Bankverbindung.

Außerdem braucht es einen IT-Partner, der die Anwendung in einem sicheren Rechenzentrum hostet und etabliert, die umfangreichen Sicherheitsmaßnahmen koordiniert, die Software an das bestehende System der Verwaltung angliedert und die besonde-

ren Security-Anforderungen des Kraftfahrt-Bundesamts sicherstellt. Diese Aufgabe übernahm das ITDZ Berlin. Der kommunale IT-Dienstleister betreibt ein Hochsicherheitsrechenzentrum, das die höchsten BSI-Anforderungen an Technik und Prozesse erfüllt und damit den idealen Rahmen für das i-Kfz-Verfahren des Landes Berlins bietet. Damit die Angliederung der Verfahrenssoftware ebenfalls den notwendigen IT-Anforderungen entspricht, informierte das ITDZ Berlin das LABO bereits in der Phase der Ausschreibung, welche technischen Voraussetzungen ein Software-Anbieter mitbringen muss, klärte die IKT-Richtlinien und stellte sicher, dass die Erweiterung des bisherigen Funktionsumfangs (wie beispielsweise Wunschkennzeichen-Online) reibungslos funktionierte.

„Man kann sagen: Als ITDZ Berlin hatten wir bei diesem Fachverfahren die Rolle eines Beraters, Umsetzers und Qualitätsprüfers“, erklärt Amin Hafez, IT-Sicherheitsberater im ITDZ Berlin. Der Berliner IT-Dienstleister beauftragte seinen Rahmenvertragspartner HiSolutions damit, wichtige Sicherheitsanforderungen des Kraftfahrt-Bundesamts (KBA) mit der i-Kfz-Architektur abzugleichen und denkbare Cyberattacken gemäß BSI-Vorgaben zu simulieren. „Auch das technische Audit lag in unserer Verantwortung, mit dem das LABO die Erfüllung aller Anforderungen des KBA nachweisen konnte.“

Als Betreiber des Fachverfahrens i-Kfz im eigenen, BSI-zertifizierten Rechenzentrum muss das ITDZ Berlin hierbei eine ganze Reihe an Sicherheitsanforderungen nachweisen. „Dazu zählt beispielsweise ein Information Management Security System, ein Notfallmanagement, die Erkennung von Sicherheitsbedrohungen sowie die richtige Reaktion darauf und vieles mehr“, erklärt Amin Hafez die umfangreichen Anforderungen, die das ITDZ Berlin erfüllen musste. (Für mehr Informationen ➔ Infobox).

Kennzeichen aus dem 3D-Drucker

Der Aufwand lohnte sich allerdings. Denn das Online-Verfahren rund um die Fahrzeuganliegen nahmen Bürgerinnen und Bürger sehr positiv auf. Die Attraktivität des Online-Fachverfahrens zeigte sich schon bald in steigenden Nutzerzahlen. In den ersten Monaten nutzten monatlich etwa 100 User das Online-Fachverfahren. In der Corona-Pandemie vervielfachte sich diese Zahl, und inzwischen werden monatlich rund 2000 Anträge abgewickelt.

Inzwischen werden monatlich rund 2000 Anträge abgewickelt.

Das Online-Verfahren i-Kfz zeigt, wie effizient die Umsetzung selbst eines großen Online-Fachverfahrens ablaufen kann. „Das ITDZ Berlin hat an diesem Erfolg einen großen Anteil“, hebt Philipp Kownatka hervor. „Es begleitete uns intensiv und umfangreich bei der Vorbereitung und überzeugte uns mit seiner kompetenten Beratung und der klaren Projektplanung. Das ITDZ Berlin reagierte immer sehr schnell und stellte den Projektstart sicher – sogar als wir in den letzten Tagen noch einmal mit einem Software-Wunsch um die Ecke kamen.“ So können Bürgerinnen und Bürger nun zu jeder Zeit und an jedem Tag ihren Behördengang rund um den eigenen fahrbaren Untersatz durchführen und sich auf die Sicherheit ihrer Daten verlassen. Auch abends um 23.49 Uhr oder sonntags um 10 Uhr mit dem Frühstücks-Croissant in der Hand. Und wer weiß: Irgendwann wird es vielleicht sogar PKW-Kennzeichen aus dem 3D-Drucker geben – dann wird man endgültig alle Autoangelegenheiten von Zuhause aus erledigen können.

„Als ITDZ Berlin hatten wir bei diesem Fachverfahren die Rolle eines Beraters, Umsetzers und Qualitätsprüfers.“

AMIN HAFEZ
IT-Sicherheitsberater im ITDZ Berlin

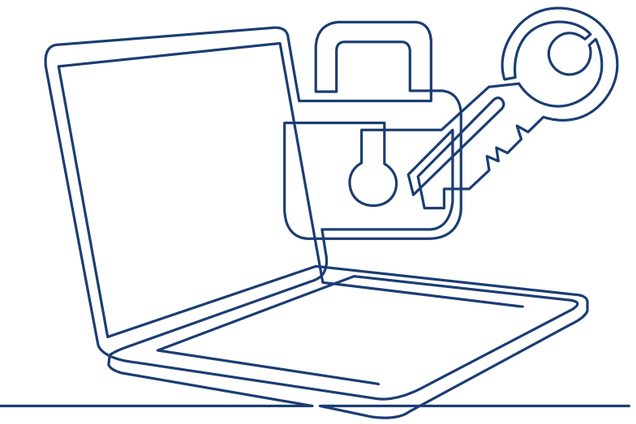
„Das ITDZ Berlin hat an diesem Erfolg einen großen Anteil.“

PHILIPP KOWNATKA
Kfz-Zulassungsbehörde Berlin

IT-Sicherheitsmaßnahmen rund um Online-Fachverfahren

Information Security Management System (ISMS)

Betreiber von Online-Fachverfahren wie das ITDZ Berlin müssen im Sinne ihrer Kunden in der Verwaltung ein Information Security Management System (ISMS) nachweisen. Ein ISMS definiert Regeln, Verfahren, Methoden und Tools, um die Informationssicherheit in einem Unternehmen oder einer Organisation zu gewährleisten, zu steuern und zu kontrollieren. So sollen Risiken, die durch den Einsatz von IT verursacht werden, identifiziert und beherrscht werden können. Die Normierung des ISMS erfolgt nach ISO-Vorgaben sowie dem IT-Grundschutz-Kompendium des Bundesamts für Sicherheit in der Informationstechnik (BSI) als Standard für Behörden. Das ITDZ Berlin betreibt ein aufwendiges und regelmäßig zertifiziertes ISMS für seine Kundinnen und Kunden in der Verwaltung.



Notfallmanagement

Das Notfallmanagement ist Teil des ISMS-Prozesses. Es stellt sicher, dass die Geschäftsprozesse der Verwaltung selbst in kritischen Situationen nicht oder nur zeitweise unterbrochen werden, damit die Verwaltung ihre Aufgaben auch bei einem größeren Schadensereignis erfüllen kann. Entsprechend analysieren IT-Expertinnen und Experten alle Aspekte eines Arbeitsprozesses, entwickeln mögliche Ereignisse, die zu einem Schaden führen können, und etablieren dafür entsprechende Gegenmaßnahmen. Zum Beispiel bedeutet das für das Hochsicherheitsrechenzentrum des ITDZ Berlin, in dem IT-gestützte Fachverfahren betrieben werden, dass dort bei einem Stromausfall ein Notbetrieb einsetzt, um die Fachverfahren verfügbar zu halten.

Erkennung von Sicherheitsbedrohungen im CDC

Über eine Million Sicherheitsbedrohungen registriert das ITDZ Berlin pro Monat für das Land Berlin. Der kommunale IT-Dienstleister erkennt und bewertet diese Angriffe in seinem Cyber Defence Center, einer Leitstelle, die sich auf die Angriffe mit Viren, Trojanern und Bots spezialisiert hat.

Professionelle Reaktion auf Cyberattacken durch das CERT

Für die Vorbeugung von und die korrekte Antwort auf Cyberangriffe führt das ITDZ Berlin das Computer Emergency Response Team (CERT) in seinen Reihen. Diese Spezialistinnen und Spezialisten für IT-Sicherheit prüfen die IT-Strukturen in der Verwaltung auf Schwachstellen und schalten sie aus. Zugleich setzen sie präventive und reaktive Maßnahmen um, um die Daten der Verwaltung nachhaltig zu schützen.

Spezielle IT-Sicherheitsmaßnahmen für das Online-Fachverfahren i-Kfz

Anforderungen des Kraftfahrt-Bundesamts

Betreiber von i-Kfz-Infrastrukturen müssen strenge Vorgaben des Kraftfahrt-Bundesamts (KBA) einhalten. Das ITDZ Berlin stellte für das Land Berlin die Einhaltung dieser Vorgaben sicher. Dazu zählen:

1 **Technische und organisatorische Sicherheitsvorgaben:** Zu den Vorgaben zählen die Implementierung eines ISMS, die Erstellung von Sicherheitskonzepten, die Etablierung eines Incident Management Systems (IT-Störungsmanagement) sowie Schulungen des Personals und der Verwaltung zum Thema Datenschutz und Informationssicherheit.

2 **Informationssicherheits-Vorgaben:** Das BSI hat einen umfangreichen Katalog mit Vorgaben erarbeitet, wie sicherheitsrelevante Prozesse bei einem Betreiber von Online-Fachverfahren einer Verwaltung zu gestalten sind. Diese Vorgaben werden regelmäßig geprüft und zertifiziert.

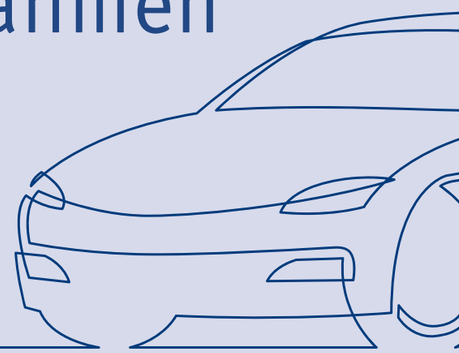
3 **Verfahrensspezifische Anforderungen:** Für gewisse Fachverfahren hat das BSI in Zusammenarbeit mit den jeweils verantwortlichen Stellen spezifische Anforderungen definiert. Im Falle von i-Kfz zählen dazu strenge Vorgaben des KBA zum Schutz der Daten sowie die Prüfung aller IT-Prozesse in Audits.

Regelmäßige Prüfungen durch externe Auditoren

Das KBA muss die Umsetzung der Vorgaben in der i-Kfz-Infrastruktur nachprüfen können. Daher werden für das LABO regelmäßige Prüfungen (Audits) der Maßnahmen durch externe Auditoren durchgeführt, die durch das ITDZ Berlin organisiert und begleitet werden. Das beinhaltet:

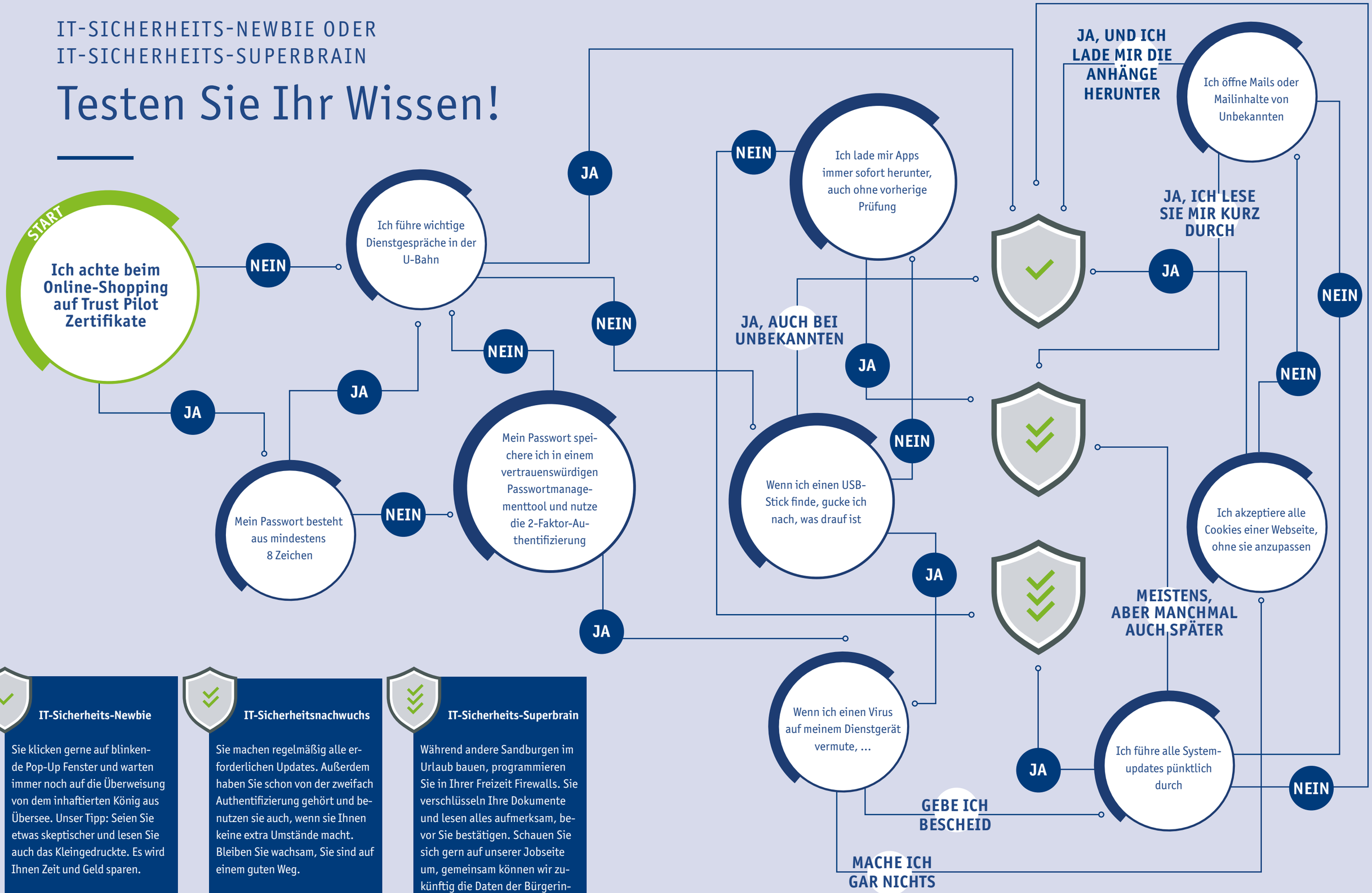
1 **IT-Sicherheitsaudits werden alle drei Jahre von unabhängigen Dritten durchgeführt und die Ergebnisse vom KBA bestätigt.** Mängel sollten innerhalb von drei Monaten behoben werden.

2 **Penetrationstests sind die Simulation von Belastungen und sicherheitskritischen Szenarien.** Sie werden alle zwei Jahre durchgeführt und prüfen, ob die Anforderungen des IT-Grundschutzes erfüllt werden und führen einen Schwachstellentest über das Internet sowie eine technische Sicherheitsüberprüfung des i-Kfz-Portals und der IT-Systeme durch.



IT-SICHERHEITS-NEWBIE ODER
IT-SICHERHEITS-SUPERBRAIN

Testen Sie Ihr Wissen!



IT-Sicherheits-Newbie

Sie klicken gerne auf blinkende Pop-Up Fenster und warten immer noch auf die Überweisung von dem inhaftierten König aus Übersee. Unser Tipp: Seien Sie etwas skeptischer und lesen Sie auch das Kleingedruckte. Es wird Ihnen Zeit und Geld sparen.

IT-Sicherheitsnachwuchs

Sie machen regelmäßig alle erforderlichen Updates. Außerdem haben Sie schon von der zweifach Authentifizierung gehört und benutzen sie auch, wenn sie Ihnen keine extra Umstände macht. Bleiben Sie wachsam, Sie sind auf einem guten Weg.

IT-Sicherheits-Superbrain

Während andere Sandburgen im Urlaub bauen, programmieren Sie in Ihrer Freizeit Firewalls. Sie verschlüsseln Ihre Dokumente und lesen alles aufmerksam, bevor Sie bestätigen. Schauen Sie sich gern auf unserer Jobseite um, gemeinsam können wir zukünftig die Daten der Bürgerinnen und Bürger beschützen.

Sie wollen mehr wissen zum Thema IT-Sicherheit? Das BSI (Bundesamt für Sicherheit in der Informationstechnik) liefert auf seiner Website aktuelle Informationen und viele Empfehlungen speziell für Verbraucherinnen und Verbraucher und bietet den Newsletter „Sicher Informiert“ an.

Sofort mehr IT-Sicherheit am Arbeitsplatz

Nicht nur die Expertinnen und Experten, alle können durch sicherheitsbewusstes Verhalten einen täglichen Beitrag zur IT-Sicherheit leisten:

1 **Wachsamkeit beim E-Mail-Empfang:** Bevor Sie Links anklicken oder Anhänge öffnen, prüfen Sie Betreff und Absenderadresse. Schauen Sie vor allem, ob die sendende Domain (hinter dem „@“) dazu passt. Die Urheber von Phishing-Mails werden immer raffinierter darin, seriöse Kontakte, wie Kolleginnen und Kollegen, nachzuahmen.

2 **Vorsicht mit alten Worddateien:** Dateien mit der Extension „.doc“ können ein Einfallstor für Schadcodes sein. Doc-Dateien aus sicherer Herkunft sollten Sie nach dem Öffnen durch „Speichern unter“ in eine aktuelle „docx“ umwandeln. Doc-Dateien in E-Mails, deren Urheber Sie nicht kennen, sollten Sie grundsätzlich nicht öffnen.

3 **An E-Mail-Verschlüsselung denken:** Vor dem Versenden von Mails mit vertraulichen oder personenbezogenen Inhalten aktivieren Sie in Outlook den Button „Verschlüsseln“ unter dem Reiter „Optionen“ und dem Untermenü „Berechtigung“.

4 **Verantwortungsvoller Umgang mit Passwörtern:** Keine Begriffe, die in Wörterbüchern zu finden sind, keine Geburtsdaten, niemals Namen Ihrer Kinder oder Haustiere. Sichere Passwörter enthalten eine Kombination aus Zahlen, Buchstaben, Groß- und Kleinschreibung und Sonderzeichen. Um sich diese zu merken, hilft ein Passwortmanager, diesen gibt es auch als Handy-App.

5 **Achtung vor Social Engineering:** Schenken Sie niemals vermeintlich vertrauenswürdigen Quellen Glauben, die Sie nach Passwörtern, Zugangsdaten oder Kontoinformationen fragen. Seriöse Firmen werden Sie nie dazu auffordern. Gehen Sie vorsichtig mit der Preisgabe von persönlichen Informationen in sozialen Medien um. Überlegen Sie genau, welche Informationen Sie in welchem Kreis offenlegen und geben Sie keine vertraulichen Informationen über Ihren Arbeitgeber preis.

6 **Zögern Sie nicht**, wenn Sie den Verdacht haben, dass bereits ein Sicherheitsereignis eingetreten ist. Wenden Sie sich umgehend an Ihren IT-Sicherheitsbeauftragten oder an Ihre IT-Stelle. Je schneller reagiert wird, umso besser kann Schaden abgewendet werden.

BESTANDEN!

Das ITDZ Berlin ist wieder BSI-zertifiziert

Die Herausforderungen für die IT-Sicherheit der öffentlichen Verwaltung sind in den letzten Jahren stark gestiegen. Die Zahl der Angriffe, Viren und Schadprogramme sowie die dadurch verursachten Schäden wachsen stetig. Rund 15 Millionen abgewehrte, potentielle Cyber-Angriffe verzeichnete das ITDZ Berlin im Jahr 2021 auf das Berliner Landesnetz (BeLa), das größte deutsche Verwaltungsstadtnetz. Eine Steigerung um fast 90 Prozent gegenüber dem Vorjahr.

Als bundesweit erster IT-Dienstleister erhielt das ITDZ Berlin 2015 das ISO 270001 Zertifikat des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für den Schutz der Daten gegen Cyber-Angriffe und die Gewährleistung einer hohen IT-Sicherheit. In diesem Frühjahr hat es erstmals die umfangreiche, alle drei Jahre vorgeschriebene Re-Zertifizierung erfolgreich bestanden. Rund 3.000 Sicherheitsmaßnahmen des ITDZ Berlin wurden umgehend geprüft und durch einen BSI-zertifizierten Auditor testiert.

Erneut BSI-zertifiziert wurden die beiden ITDZ-Rechenzentren mit virtuellen und physischen Servern, die Netze und Netzwerktechnik zur verschlüsselten Kommunikation über das Berliner Landesnetz, sowie die IKT-Basisinfrastruktur und zentrale IKT-Dienste für die Berliner Verwaltung. Gegenstand der Zertifizierung waren darüber hinaus auch die private BerlinCloud, der standardisierte Arbeitsplatzrechner BerlinPC und das Notfallmanagement des ITDZ Berlin.

„Das Vertrauen der Berliner Bürgerinnen und Bürger in zertifizierte IT-Sicherheit und den Schutz der sensiblen Daten bilden das Fundament für moderne, digitale Verwaltungsdienstleistungen“, sagt Marc Böttcher, Vorstand des ITDZ Berlin. „Erneut hat das BSI bestätigt, dass diese Daten im ITDZ Berlin nach höchsten IT-Sicherheitsstandards übertragen, gespeichert und geschützt werden.“

„Das Vertrauen der Berliner Bürgerinnen und Bürger in zertifizierte IT-Sicherheit und den Schutz der sensiblen Daten bilden das Fundament für moderne, digitale Verwaltungsdienstleistungen.“

MARC BÖTTCHER, Vorstand des ITDZ Berlin

SpirIT

Einblicke und Persönliches
aus dem ITDZ Berlin

EINER VON UNS

„Nervös machen mich nur Flauten“

Seit wann sind Sie für das ITDZ Berlin tätig?
Vor mehr als 20 Jahren, 2001, bin ich zum ITDZ Berlin gekommen. Als Diplom-Ingenieur für Nachrichtentechnik war ich jahrelang in der Entwicklung für Satellitentechnik tätig und habe dann den Sprung in die Verwaltung gemacht.

Was genau sind Ihre Aufgaben?
Als Informationssicherheitsbeauftragter sind meine Aufgaben nach dem BSI-Grundschutz geregelt. Kurz gesagt, initiiere und steuere ich Informationssicherheit im ITDZ Berlin. Beispielsweise fallen Revisionen/Audits im Themenbereich der Informationssicherheit in meinen Verantwortungsbereich, worüber ich unser aktuelles Informationssicherheitsniveau überprüfe. Ich leite das Sicherheitsmanagementteam, denn jeder Bereich stellt seine eigenen Sicherheitsbeauftragten, und steuere die Zusammenarbeit mit dem BSI zur Informationssicherheit.

Was reizt Sie besonders an Ihrer Beschäftigung?
Das Spannende an meiner Tätigkeit? Es wird nie langweilig, denn das Themengebiet Informationssicherheit ist extrem dynamisch! 2005 kannten wir Firewalls und Anti-Viren-Scanner – heute ist es die verhaltensbasierte Schadsoftwareerkennung, auf die wir unseren Fokus legen. „Verhaltensbasiert“ bezieht sich dabei übrigens auf das Verhalten der Software. Wir analysieren, auf welchen Maschinen die Schadsoftware läuft und leiten Maßnahmen zur Eindämmung ein.

Karsten Pirschel

ist seit 2013 Informationssicherheitsbeauftragter des ITDZ Berlin.

Außerdem ist IT-Sicherheit mehr als je zuvor ein gesellschaftliches Thema, mit dem sich jeder auseinandersetzen muss wie mit der Impfpflicht. Wo liegen die Server meiner Daten? Wer hat darauf Zugriff und kann sie überwachen? Liegen meine Daten außerhalb der EU und gibt es Gesetze, die fremden Staaten den Zugriff auf meine Daten geben? Wie gehe ich selbst mit meinen Daten um? Jede und jeder Einzelne muss sich mit solchen Fragen auseinandersetzen – und wir als IT-Dienstleister des Landes Berlin in aller Breite und der maximal möglichen Tiefe. Nur so können wir unserer Verantwortung für die Daten aller Berlinerinnen und Berliner gerecht werden.

Das ITDZ Berlin kommt einer Festung für Daten gleich. Woraus besteht diese?
Ja, das stimmt. Unsere „Burg" besteht aus dem eigenen Landesnetz, den beiden Landesrechenzentren und der Hard- und Software bei den Kundinnen und Kunden. Hier lagern Verwaltungsdaten der Berliner Bürgerinnen und Bürger, und ein trojanischer oder anderweitig sicherheitsgefährdender Zugriff darauf wäre fatal. Entsprechend hoch ist das Sicherheitsniveau aller Prozesse und der IT-Standardinfrastruktur, die in der Verantwortung des ITDZ Berlin liegen.

Was war Ihr spannendster ITDZ Berlin-Moment?
Als erstes fällt mir die BSI-Zertifizierung 2015 ein. Als erste Institution wurden wir damals nach dem neuen, modernisierten BSI-Grundschutz zertifiziert und konnten dies 2022 wiederholen. Weitere Meilensteine waren die Modernisierung unserer beiden Rechenzentren, das High Secure Data-Center (HSDC) und das Secure Data-Center (SDC). An diesen geheimen Orten gewährleistet das ITDZ Berlin die Sicherheit von Daten und Anwendungen der Landesverwaltung.

Bereits vor Jahren haben wir uns dazu entschieden, eine Private Cloud im eigenen Rechenzentrum für die Berliner Verwaltung anzubieten, die die Anforderungen an die IT-Sicherheit und das Berliner Datenschutzgesetz erfüllt – die ganze Cloud-Strategie finde ich extrem spannend.

Bei so vielen potentiellen Gefährdungen im Berufsalltag – kann Sie persönlich noch etwas nervös machen?
Eine Flaute.

Das müssen Sie erklären!
Mit dem Eintritt in das ITDZ Berlin habe ich damals auch mit dem Kite-Surfen begonnen. Wenn Sie mit 40-50km/h auf das Meer hinausgleiten und dann plötzlich der Wind weg ist, haben Sie ein Problem.

KARSTEN PIRSCHEL, der passionierte Sportler steigt in seine Freizeit auch gerne mal aufs elektrische Einrad.

„IT-Sicherheit ist mehr als je zuvor ein gesellschaftliches Thema, mit dem sich jeder auseinandersetzen muss."

KARSTEN PIRSCHEL

Was ist Ihr Lieblingsort in Berlin/Brandenburg?
So viel sei gesagt, ich habe einen „Secret Spot" an einem Brandenburger See. Wenn ich den Namen jetzt nenne, bin ich da vielleicht bald nicht mehr alleine (lacht). Der einzige See in Brandenburg, wo Kite-Surfen erlaubt ist, ist übrigens der Scharmützelsee in Bad Saarow.

Wie schalten Sie nach einem Arbeitstag ab?
Mein Weg vom Büro nach Hause führt am Tempelhofer Feld vorbei – ein friedlicher, fast schon magischer Ort in Berlin. Da kann ich auch gut eine Runde „Landboard-Kiten", denn an einen See, geschweige denn ans Meer, schaffe ich es unter der Woche nicht.

Vielen Dank für dieses Gespräch.

AUF DEN PUNKT

Kurzmeldungen

Happy Birthday: 10 Jahre Diversity Tag!

Unter dem Motto „Let's celebrate Diversity" feierte der Deutsche Diversity-Tag, initiiert von der Charta der Vielfalt, in diesem Jahr am 31.05.2022 10-jähriges Jubiläum. Das ITDZ Berlin als unterzeichnendes Unternehmen der Charta feierte mit – mit Online- und vor Ort-Angeboten für Mitarbeitende sowie Aktionen auf der Website und Instagram.
Das ITDZ Berlin hat sich dazu bekannt, Vielfalt zu fördern und Diskriminierung entgegenzuwirken und nimmt die gesellschaftliche Verantwortung an. Als kommunales Unternehmen in einer Stadt, die von Vielfalt geprägt ist, ist es der Anspruch des Hauses, möglichst nah an den Bürgerinnen und Bürgern Berlins zu sein und Diversity auch im ITDZ Berlin abzubilden.

Das ITDZ Berlin hilft in der Ukraine-Krise

Das ITDZ Berlin unterstützt das Land Berlin bei der schnellen Hilfe für geflüchtete Menschen aus der Ukraine und bringt dabei seine Expertise in verschiedene Bereiche ein. Eine zentrale Rolle nimmt in diesem Zusammenhang die eigens eingerichtete Service-Hotline ein, die durch das ITDZ Berlin betrieben und in vier Sprachen bedient wird. Geflüchtete und Helfende erhalten hier die wichtigsten Antworten zu Unterkunft, Registrierung, Visum und Aufenthaltsrecht. Darüber hinaus hat das ITDZ das Ankunftszentrum in Reinickendorf, den Krisenstabsraum im Landesamt für Flüchtlingsangelegenheiten und das Registrierungszentrum in Tegel technisch ausgerüstet und mit aufgebaut. Die Einrichtung eines digitalen Antrags für Aufenthaltsgenehmigungen und eine Online-Termin-Vergabe für Geflüchtete, waren zwei weitere wichtige Leistungen, mit denen das ITDZ Berlin seinen Teil zur Hilfe für die Geflüchteten beiträgt.

Breitbandanbindung der Berliner Schulen

Das Land Berlin hat sein Programm „Breitband- und WLAN-Ausbau der Berliner Schulen (BWAS)" gestartet. Darüber werden bis Ende 2025 alle rund 800 Standorte der allgemeinbildenden Schulen in Berlin mit schnellem Internet bis in die Klassenzimmer ausgestattet. Die Umsetzung des landesweiten Programms erfolgt unter der Leitung des ITDZ Berlin und startete mit dem Glasfaseranschluss von 12 Prototypen-Schulen – je ein Schulstandort pro Bezirk.

Die Zukunft im Blick – Das ITDZ Berlin baut auf Nachhaltigkeit

Das ITDZ Berlin kommt seiner eigenen Verantwortung als energieverbrauchender IT-Dienstleister nach und arbeitet aktiv am Landesziel der klimaneutralen Hauptstadt mit.

Als zentraler IT-Dienstleister haben wir uns in einer Klimaschutzvereinbarung bis 2030 zu einer Einsparung unserer direkten CO2-Emissionen von 33 Prozent gegenüber dem Jahr 2019 verpflichtet. Verbleibende direkte Emissionen werden kompensiert. Indirekte CO2-Emissionen, also Emissionen, die außerhalb des ITDZ Berlin bei der Erzeugung gelieferter Energieträger entstehen, sollen bis 2030 um mindestens 13 Prozent reduziert werden. Schon vor der Unterzeichnung der Klimaschutzvereinbarung haben wir uns auf den Weg zu mehr Nachhaltigkeit gemacht. Das ITDZ hat beispielsweise seine 2020 direkt verursachten CO2-Emissionen gemeinsam mit der Umweltorganisation PRIMAKLIMA kompensiert. Durch eine Spende, die in die Aufforstungsprogramme der Organisation fließt, konnten wir insgesamt 72 Tonnen CO2 ausgleichen.

Bringen Sie Ihr IT-Sicherheitswissen auf den neuesten Stand

Sicherheit entsteht, wenn alle mitmachen! Das Behörden IT-Sicherheitstraining (BITS) ist in einer neuen Version verfügbar und richtet sich an alle Mitarbeitenden der Berliner Verwaltung.

Das BITS soll das Sicherheitsbewusstsein der Mitarbeitenden im öffentlichen Dienst erhöhen, indem es für Gefahren und Bedrohungen sensibilisiert, grundlegendes Wissen zu IT-Sicherheitsthemen vermittelt und konkrete Handlungsempfehlungen ausspricht. Es eignet sich also sowohl zum Einstieg in das Thema Informationssicherheit als auch zum Auffrischen bereits vorhandener Kenntnisse. Die Lerngeschwindigkeit kann von den Nutzenden selbst bestimmt werden. Über die Seite des Berlin-CERT im Berliner Landesnetz ist das BITS – für Kundinnen und Kunden des ITDZ Berlin – in der neuen Version 6.0.2 erreichbar: https://bits.berlin-cert.verwalt-berlin.de/.

Buchtipps zur IT-Sicherheit

Sie schauen schon den ganzen Tag auf den Bildschirm und möchten zur Abwechslung mal wieder ein echtes Buch in den Händen halten? Kein Problem! Für alle, die das gedruckte Wort bevorzugen haben wir drei aktuelle Buchtipps zusammengestellt:

„Hacking & IT-Security für Einsteiger: Der leichte Weg zum IT-Security-Experten“ von Max Engelhardt, 542 Seiten, BMU Verlag, 19,99€

„Hacking & Security: Das umfassende Hacking-Handbuch mit über 1.000 Seiten Profiwissen.“ 2. aktualisierte Auflage von Michael Kofler & Klaus Gebeshuber & weitere, 1124 Seiten, Rheinwerk Verlag, 49,90€

“IT-Sicherheit: Technologien und Best Practices für die Umsetzung im Unternehmen“, 1. Edition, von Michael Lang, Hans Löhr, Carl Hanser Verlag GmbH & Co. KG, 39,99€

Gesunde und schnelle Cookies – im leckeren Sinn

Was wäre ein gutes Magazin ohne ein Rezept, das thematisch zum Heft passt? Diese Cookies werden Ihre Pausen versüßen und garantiert nur wenige Krümel statt sensibler Daten hinterlassen.

Auswahl bestätigen

Zutaten:

2 sehr reife Bananen
160 Gramm zarte Haferflocken

Optionen zum Verfeinern:
80 Gramm Trockenfrüchte wie Pflaumen, Rosinen oder Aprikosen
2 Esslöffel Erdnussbutter crunchy
Zimt
Vanille
dunkle Schokodrops

Hab ich noch! auf die Liste

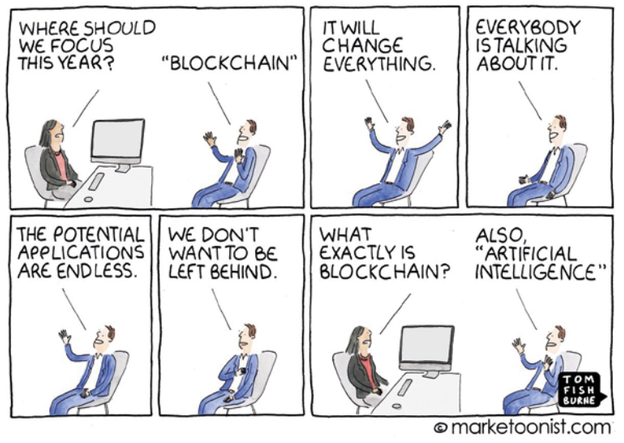
Zubereitung:

Ofen auf 175 Grad vorheizen. Bananen zerdrücken und alle Zutaten miteinander vermischen.
Kleine Kugeln formen und auf dem Backblech flach drücken.
Cookies rund 15 Minuten backen und dann abkühlen lassen.

Viel Spaß beim Genießen der gleichermaßen daten- und gelingsicheren Cookies

DAS LETZTE!

Humorvolles aus der Welt der IT



**Sie haben Anmerkungen, Themenwünsche oder möchten uns Ihre Meinung sagen?
Schreiben Sie gern an
redaktion@itdz-berlin.de**

Sind Sie neugierig geworden?

Dann nutzen Sie auch unsere weiteren Kanäle für Informationen rund um das IT-Dienstleistungszentrum Berlin!

Unsere SOC-Premiere als Film – jetzt anschauen!

www.itdz-berlin.de

instagram.com/itdzberlin

Landesbeschäftigtenportal Berlin: b.intern.de/wb/itdz

(exklusiv für Kundinnen und Kunden)

Sichern Sie sich **bITDZ & bytes** im kostenfreien Abo!

www.itdz-berlin.de/aktuelles/bitdz-bytes/

ITDZ BERLIN