QUELLTEXT

MICROMATA-MAGAZIN 02/2021

MICROMATA

GANZHEITLICHE IT-SECURITY
So sichern wir Ihre Software-Systeme
› AB SEITE 10

DEMOKRATIE IM DIGITALEN ZEITALTER
Sicher und barrierefrei wählen mit POLYAS
› SEITE 6

AUS 1 MACH 2
Manchmal haben wir schon, was wir brauchen
› SEITE 8

50 JAHRE UNI KASSEL
Micromata finanziert drei Deutschlandstipendien
› SEITE 26

Die Schöpferin des aktuellen Quelltext-Titelbildes ist Clara Höferlin. Unsere Werkstudentin im Bereich UX ist also nicht nur in Sachen Software-Design unterwegs, sondern hat auch ein Händchen für Illustration. Finden wir super – und sind gespannt, welche verborgenen Talente noch in ihr schlummern...

In jeder Quelltext-Ausgabe präsentieren wir einen Künstler oder eine Künstlerin unseres Herzens. Als Unterstützung der freien Kunst und Verneigung vor der Kreativität der Anderen.

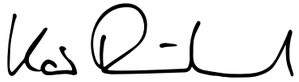
AUF EIN WORT

Liebe Leserinnen und Leser,
wir leben in bewegten Zeiten. Mit einer Vielzahl an neuen oder noch nicht bewältigten Herausforderungen. Egal, ob Klimawandel, Corona-Pandemie oder Digitalisierung: Es sind Lösungen gefragt. Als Softwarehaus mit Schwerpunkt auf passgenauer Industriesoftware wissen wir, dass es maßgeschneiderte Lösungen selten von der Stange gibt – und dass gute Ideen nicht nur für den Moment geboren sein dürfen, sondern mit den Erfordernissen der Zukunft mitskalieren sollten.

Das bedeutet, dass wir auch im Bereich IT-Security ganzheitlich denken und handeln. Unser Anspruch: der Gefahr nicht auf den Fersen, sondern mindestens einen Schritt voraus zu sein. Wie wir das machen, erläutern wir im Titelthema ab Seite 10.

Natürlich wissen wir, dass es neben Sicherheit auch an Werten wie Mut, Optimismus und Kreativität nicht mangeln darf, um gute Antworten auf die drängenden Fragen der Zeit zu finden. Deshalb wünsche ich Ihnen genau das – für die verbleibenden Wochen dieses Jahres ebenso wie für ein vielversprechendes 2022. Wir freuen uns auf eine weiterhin lösungsorientierte Zusammenarbeit im nächsten Jahr!

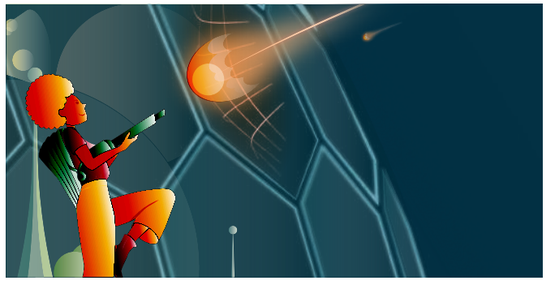
Viel Spaß beim Lesen wünscht Ihnen Ihr



Ihr Kai Reinhard

\TABLEOFCONTENTS

QUELLTEXT
MICROMATA-MAGAZIN
02/2021



Ganzheitliche IT-Security

So sichern wir Ihre Software-Systeme.

› SEITE 10

Auf eine Tasse Java mit ...

Florian Heinecke, Informationssicherheit & Datenschutz bei Micromata.

› SEITE 14

JUGH-Tagebuch

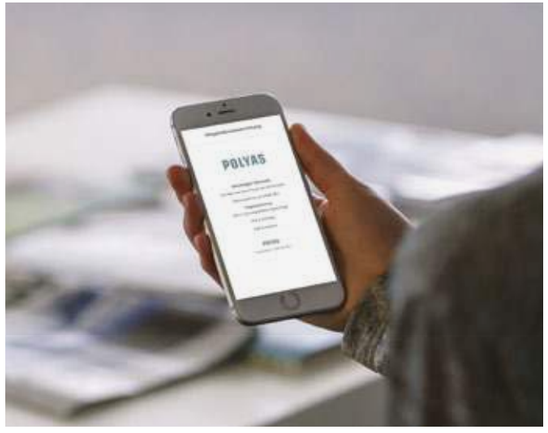
Das war los bei der Java User Group Hessen im zweiten Halbjahr 2021.

› SEITE 18

ITSMKS

Schlaglichter aus der Arbeit des IT-Security Meetups Kassel.

› SEITE 20



Digitale Demokratie

Sicher und barrierefrei wählen mit POLYAS.

› SEITE 6

50 Jahre Uni Kassel

Micromata finanziert 3 Deutschlandstipendien für Informatik-Studierende.

› SEITE 26

3 Auf ein Wort

AUS DEN PROJEKTEN

6 Demokratie im digitalen Zeitalter

8 Aus 1 mach 2

TITELTHEMA

10 Ganzheitliche IT-Security

14 Auf eine Tasse Java mit ...

MODERN TALKING

16 Vorsicht giftige Post!

17 Clean Code steigert Softwaresicherheit

17 Spielerische Sicherheit

KNOW-HOW-TRANSFER

18 JUGH-Tagebuch

20 IT-Security Meetup Kassel

22 Hacktoberfest 2021

24 Codeweek Kassel 2021

MICROMATA NEWS

25 Alexander Podlich ist neuer Gesellschafter

26 50 Jahre Uni Kassel

Digitale Demokratie

Wie POLYAS das Wählen sicherer und barrierefreier macht

IT-Security ist erfolgsentscheidend. Das gilt auch für das Online-Wahlsystem POLYAS, das einst als Forschungsprojekt von Micromata begann und seit 2012 als eigenständige GmbH mit Hauptsitz in Kassel und einer Zweigstelle in Berlin sehr erfolgreich ist. Noch heute sind sich die Softwareentwickler von Micromata und POLYAS eng verbunden und arbeiten weiterhin gemeinsam daran, das System zu verfeinern und unsere Demokratie noch digitaler zu machen.

Dazu gehört unter anderem ein hohes Sicherheitsniveau, dass neben Barrierefreiheit und Nutzerfreundlichkeit vielleicht der wichtigste USP der Online-Wahlsoftware ist. Alles davon kristallisiert sich um den Rechtsanspruch der Wählenden auf freie, gleiche, unmittelbare und geheime Wahlen, die auch bei einer digitalen Wahl unter allen Umständen gewährleistet sein müssen. Ansprüche, denen POLYAS durch eine intelligente Systemarchitektur gerecht wird.

Das Standard-Setup umfasst:

- räumliche und organisatorische Trennung von Wählerverzeichnis und Wahlurne
- sichere Identifizierung der Wahlberechtigten, z. B. durch Zwei-Faktor-Authentifizierung
- Anmeldung via PIN/TAN, Personalausweis oder das Portal des Wahlveranstalters
- moderne kryptographische Verfahren zur Wahrung des Wahlgeheimnisses
- Transparenz gegenüber möglichen Manipulationsversuchen, u. a. mithilfe von Prüfsummen
- regelmäßige Penetrationstests im Hinblick auf neue Angriffsvektoren (zum Beispiel Denial-of-Service-Attacken)

Dabei hat sich das Sicherheitskonzept hinter POLYAS über die Jahre stetig weiterentwickelt – und tut es noch immer. Während das klassische Set-up vom BSI schon lange zertifiziert ist, tüfteln POLYAS und Micromata auch weiterhin an neuen Technologien und Tools, um das System noch besser zu machen und mit der digitalen Entwicklung und den unterschiedlichen Bedrohungen mitzuskalieren.

POLYAS vs. Briefwahl oder Wahllokal

Welche Art zu wählen die sicherste ist, hängt immer von den Begleitumständen und dem Umfeld einer Wahl ab. In Deutschland etwa gilt die Urnenwahl als sehr sicher, weil sie in eine funktionsfähige Demokratie eingebunden ist und das Prozedere kaum Manipulationsmöglichkeiten zulässt. Anders die Briefwahl: Dort lauern zwischen Stimmabgabe und Auszählung gleich mehrere Sicherheitslücken auf dem Weg – angefangen beim der Zustellung der Wahlunterlagen über deren Rückweg, welche beide keinen Nachweis über den sicheren Eingang beim Empfänger vorsehen, bis hin zur Lagerung der Briefe vor der Auszählung. Demgegenüber bieten Online-Wahlsysteme wie POLYAS ein deutlich höheres Sicherheitsniveau, weil die Stimme ohne Umwege in der Urne landet und Manipulationsversuche sofort transparent gemacht werden können. Auch in Ländern mit weniger gefestigten Demokratien kann POLYAS deshalb eine sichere Alternative zur Briefwahl sein.

Barrierefreiheit

Die Kernidee von Wahlen ist Teilhabe. Ihr Ideal ist, dass möglichst viele Menschen an der politischen Willensbildung partizipieren. Im Alltag kann dieses Ideal an Grenzen stoßen – etwa ein zu weiter Weg ins Wahllokal oder eine eingeschränkte Mobilität. Auch hier kann POLYAS ein sinnvoller Beitrag zu mehr Beteiligung durch mehr Barrierefreiheit sein.

Den Machern von POLYAS geht es bei all dem nicht um eine radikale Abschaffung etablierter Wahlformen. Sie verstehen ihr Angebot als Ergänzung für alle, die sich im digitalen Raum zuhause fühlen und als notwendige Maßnahme, die Demokratie am technischen Fortschritt zu beteiligen.

Fazit

Seit POLYAS Ende der 90er Jahre erstmals als Software das Licht der Welt erblickte und 2012 erfolgreich ausgegründet wurde, haben zahlreiche Vereine, Verbände, Parteien, Unternehmen und Institutionen ihre Kandidaten und Gremien erfolgreich online gewählt. Jede Wahl war für das System gleichzeitig ein Herz-und-Nieren-Test, der zum heutigen Niveau der Software beigetragen hat. Der nächste Schritt sind politische Wahlen, für die sich POLYAS technisch wie fachlich gerüstet sieht. Erstes großes Projekt in diesem Bereich: die Sozialwahlen 2023. />

Empfehlung

„Wann können wir den Bundestag online wählen, Kai Reinhard?“

Tech-Podcast STRG + ALT + ENTF
des BITKOM vom 13. September 2021

Aus 1 mach 2

Manchmal haben wir schon, was wir brauchen – wir müssen nur hinsehen.

Es muss nicht immer das ganz große Rad gedreht werden, um eine perfekte Lösung zu erzielen. Im Gegenteil – das große Rad kann auch hinderlich sein, wenn es um die schnelle Umsetzung einer schlanken, leichtgewichtigen Anwendung geht.

Beispiel: Die Kasseler Verkehrs- und Versorgungs GmbH (KVV) war auf der Suche nach einem passenden Tool, das die Redaktion von News im hauseigenen Intranet und der Mitarbeiter-App kombiniert und gleichzeitig als Analysetool dient. Die üblichen Verdächtigen unter den CMS – WordPress oder Typo3 – bringen zwar eine Menge Features mit, waren aber genau deshalb zu komplex in der Bedienung und wollten auch sonst nicht recht zu den Bedarfen und Wünschen passen.

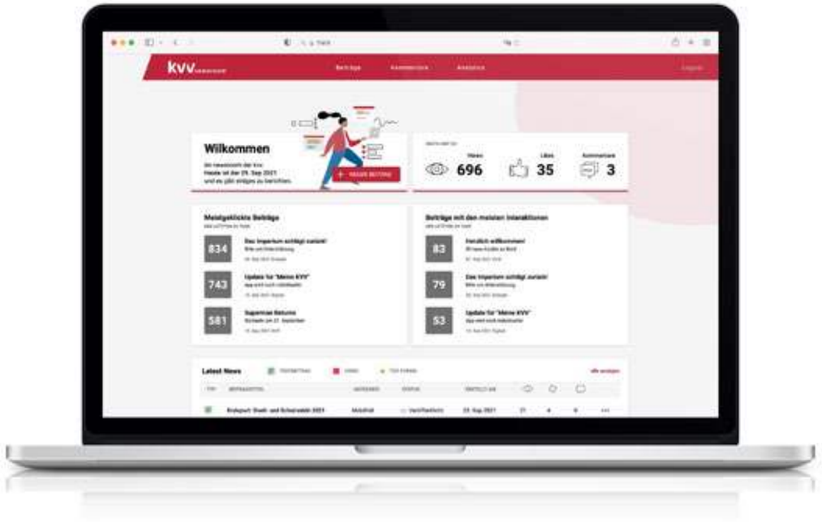
Die Lösung: TWIX!

Was haben wir also gemacht? Wir haben kurzerhand die Serveranwendung der letzten gemeinsamen Entwicklung – der KVV App – geklont. Architektur und Technologiestack blieben die gleichen, so dass bei der Entwicklung die Einarbeitung eingespart wurde. Viel Code konnte zudem einfach wiederverwendet werden und die Anforderungen an Dashboard, Newserstellung, Kommentarmoderation und Analytics konnten voll damit erfüllt werden. Entstanden ist so eine Zwillingsanwendung, die optimal zu den gestellten Ansprüchen passt und bei der Kommunikation mit der App perfekt zusammenarbeitet.

Im Frontend haben wir eine schlanke React-Anwendung mit ansprechendem Design und intuitiver Nutzung hinzugefügt. Es sind genau die Funktionen vorhanden, die gebraucht werden und keine überflüssigen Einstellungsmöglichkeiten. Darüber hinaus bietet die Anwendung Möglichkeiten, weitere Wünsche der KVV in zukünftigen Releases wahrzumachen, beispielsweise einen Planungskalender für Artikel oder eine Erweiterung der Analysefunktion. />

„Am Ende war das Vorgehen für beide Seiten das Beste: Wir hatten mehr Spaß dabei, unseren eigenen Code wiederzuverwenden, als ein fertiges CMS anzupassen – und wir hatten einfach Lust darauf, ein eigenes Redaktionstool zu bauen. Und die KVV hat für wenig Geld eine Individualsoftware bekommen, die ihre Anforderungen voll erfüllt."

ANNA KLINGAUF
Softwareentwicklerin



- Kostenrahmen: nur 70 Leistungstage (Umsetzung)
- zzgl. Vorbereitungsphase/ Workshop

„Mit Twix hat die Micromata für uns ein Redaktionstool entwickelt, das genau unseren Bedarf an eine zeitgemäße und flexible News-Redaktion erfüllt. Zeitgleich sehen wir nun auf einen Blick, welche Beiträge unsere Kolleginnen und Kollegen lesen und wie sie per Like oder Kommentar darauf reagieren. Die gemeinsame Arbeit an Twix hat uns viel Spaß gemacht, wir wurden von den Entwicklern bei jedem Schritt mitgenommen und professionell beraten.

STEFANIE GUNDLACH
Referentin Interne Kommunikation KVV

Ganzheitliche IT-Security

So sichern wir Ihre Software-Systeme

Die Entwicklungen im Bereich der Cyberkriminalität zeigen, dass wir uns schützen sollten. Allein in Deutschland lag die Anzahl der Opfer von Hackerangriffen im Jahr 2019 bei 17,7 Millionen Fällen*, der finanzielle Schaden bei 100 Milliarden Euro. Heute, zwei Jahre später, liegen zwar noch keine offiziellen Zahlen vor, die Lage dürfte aber weiterhin ernst sein.**

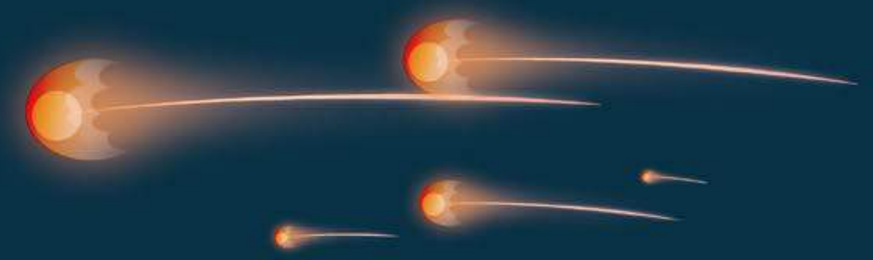
Es ist also nicht nur Vorsicht geboten, sondern Vorsorge. Es reicht nicht mehr aus, sichere Verbindungen herzustellen und Antivirensoftware zu installieren. Auch die Verschlüsselung von Daten bietet allein keinen ausreichenden Schutz. Vielmehr muss IT-Security heute ganzheitlich gedacht sein – als erklärtes Ziel und integraler Baustein jedes einzelnen Software-Projektes – von Anfang an, entlang des gesamten Software-Life-Cycles.

Reputation und Markterfolg

Denn IT-Sicherheit zahlt sich unmittelbar auf die Reputation von Unternehmen aus. Wer seine Systeme zu schützen weiß, schützt auch deren Nutzer: Mitarbeiter, Partner, Kunden. Wer deren Daten „verliert“, verliert auch deren Vertrauen in die eigene digitale Kompetenz.

Um fair zu bleiben: Letzte Gewissheit bzw. ultimative Sicherheit gibt es nicht. Wir alle können Zielscheibe solcher Angriffe werden. Was es aber gibt, ist die Verantwortung, hohe Sicherheitsstandards zu setzen und den Erfolg von Cyberattacken möglichst unwahrscheinlich zu machen bzw. deren Schaden auf ein Minimum zu reduzieren.

Wir bei Micromata stehen für einen holistischen Sicherheitsansatz – von A wie Anforderungsanalyse bis Z wie ein zukunftsfähiges Security-Konzept. Die wiederholte Zertifizierung durch den Verband der Automobilindustrie (VDA) bestätigt uns in diesem Kurs:



TISAX***

Das TISAX-Zertifikat des VDA basiert auf einem verbindlichen Kriterienkatalog, der auf Grundlage der Industrienorm ISO/IEC 27001 entwickelt wurde. Der TISAX-Zertifizierung geht eine Inspektion durch eine Prüfstelle voraus, die dafür von der European Network Exchange Association, dem Verbund Europäischer Automobilhersteller, -Zulieferer und Verbände, akkreditiert wurde. Geprüft wird neben der Sicherheit der eingesetzten Tools und Technologien auch die genutzte Infrastruktur und Hardware sowie die operativen Prozesse, die Handlungsfähigkeit im Angriffsfall und das Verhalten der Mitarbeiter (Security Compliance/Policy, Sicherheitsschulungen etc.)

Was wir tun, um die hohen Security Standards von TISAX auch in Projekten für andere Branchen sicherzustellen, wird im Folgenden kurz umrissen.

Best Practices

Von allen Sicherheitslücken gelten SQL Injections als die häufigsten und gefährlichsten, doch auch NoSQL Injections, CSRF und Brute-Force-Attacken sind reale Bedrohungen für Webanwendungen im Netz. Um diesen zu begegnen, härten wir unsere Infrastruktur mithilfe erprobter Best Practices, die für jedes Szenario maßgeschneidert sind. Dabei spielen neben den Standards der jeweiligen Kunden auch die Empfehlungen des OWASP eine Rolle, die weltweit führend bei der Identifikation und Beseitigung von Sicherheitslücken sind.

Pentesting

Wir können gar nicht deutlich genug betonen, wie wichtig ein professionelles Pentesting ist. Je nach Business Case des Kunden kann dies ganz individuell zugeschnitten werden. Unser Know-how reicht dabei von der Implementierung einer validen Testumgebung über klassische Black- und Whiteboxanalysen bzw. Analysen des Softwarecodes bis hin zu praktischen Handlungsempfehlungen zur schnellen Schließung von Sicherheitslücken. Ob die Tests automatisiert oder manuell durchgeführt werden, hängt vom jeweiligen Auftrag ab und kann gemischt sein. In jedem Fall wird die Sicherheit von Webanwendungen durch ein sorgfältiges Pentesting deutlich erhöht.

Safety by Design

Auch ein gutes Nutzungsdesign kann nachweislich zur Datensicherheit in Webanwendungen beitragen – insbesondere im Hinblick auf die Authentifizierung. Bei aller Verantwortung des Einzelnen für ein sicheres Verhalten im Netz, spricht es durchaus für eine gute Kundenorientierung, die Nutzer:innen nicht völlig damit allein zu lassen. Denn wie die Erfahrung zeigt, ist es von der Einsicht in die Notwendigkeit bis zur praktischen Umsetzung sicherer Routinen ein langer Weg

– wenn dieser denn überhaupt eingeschlagen wird. Hier ein paar Beispiele, was Webanbieter für die Sicherheit ihrer Kundschaft tun können – zumindest so lange das Passwort-Zeitalter noch andauert. Ob und in welchem Umfang wir dies umsetzen, hängt vom Wunsch des jeweiligen Kunden ab, möglich ist es aber immer:

- Passwörter als Hashes zu speichern dürfte heute selbstverständlich sein[1]
- Passwort-Generator ins Registrierungsformular integrieren[2]
- Passwort bei jeder Anmeldung automatisiert auf Leaks überprüfen[3]
- Auf Single-Sign-On grundsätzlich verzichten[4]
- Multi-Faktor-Identifizierung als verbindlichen Standard festlegen[5]
- Sinnvolle Sicherheitsabfragen stellen od. durch vertrauenswürdige Faktoren ersetzen[6]
- Automatisierte E-Mails durch sichere Alternativen ersetzen[7]

Die gute Nachricht: Das Passwort-Zeitalter neigt sich seinem Ende entgegen. Auch wir erproben heute schon Ansätze, wie künftig darauf verzichtet werden kann. So gibt es bereits vielversprechende Lösungen wie die WebAuthn-API als Teil der FIDO2-Spezifikationen. Dazu werden Sie künftig noch von uns hören.

[1] So sind sie besser vor Leaks geschützt

[2] Ist die Nutzung freiwillig, wird sie eine Seltenheit bleiben

[3] z. B. mithilfe von Datenbanken auf Basis von haveibeenpwned.de. Falls ein Leak vorliegt, dann automatisierte Rückmeldung an die/den Betroffene:n

[4] Auch wenn die Optionen „Mit Google oder Facebook anmelden" attraktiv für den Anbieter und bequem für den Nutzer ist, gibt letzter damit den Generalschlüssel für mehrere Accounts aus der Hand

[5] Noch immer hat sich 2FA nicht flächendeckend durchgesetzt

[6] Der Name des Haustiers od. das Geburtsdatum sind etwa bei Doxing-Angriffen viel zu leicht zu erraten

[7] Gefälschte und verseuchte E-Mails sind die Haupteinfallstore für Phishing und Co. Wer sicher gehen will, verzichtet darauf.

IT-Security-Team

Das IT-Security-Team von Micromata dürfte den meisten unserer Leser bekannt sein: Es sorgt dafür, dass wir uns stets am Puls der security-technischen Entwicklung bewegen. Dazu beobachten sie nicht nur ständig die Entwicklung der Sicherheitslage im Netz mithilfe der einschlägigen OWASP-Publikationen, sondern wählen auch passende Instrumente zur Vermeidung und Schließung von Sicherheitslükken, führen Schulungen für Kunden und Mitarbeiter durch und kümmern sich um die Zertifizierungen auf diesem Gebiet.

Security Champions

Um das IT-Security-Team in seiner Arbeit zu unterstützen, gibt es seit 2019 in jedem Projektteam so genannte Security Champions, die unser Security-Know-how noch effizienter in den Teams verankern – seien dies bestimmte Vorgehensweisen bei der Programmierung,

Prüfung und Auswahl konkreter Technologien oder die Beratung unserer Kunden zur Sache. Da sie unmittelbar in den Projekten tätig sind, können sie mögliche Incidents zudem schneller erkennen und die Reaktionszeit weiter signifikant verkürzen.

Das IT-Security Meetup Kassel

Das IT-Security Meetup Kassel ist ein Netzwerk von Experten und Interessierten zum Thema IT-Sicherheit. Eingeladen sind alle, die sich beruflich oder aus persönlichem Interesse mit Fragen der IT-Sicherheit auseinandersetzen und in einen fachlichen Austausch mit Gleichgesinnten treten wollen. Seit seiner Gründung hat sich das ITSMKS zu einer Institution mit internationalen Speakern und Publikum entwickelt, von deren lebendigem Know-how-Transfer auch unsere Kunden profitieren. Micromata hat das ITSMKS 2016 mit ins Leben gerufen und ist seither dessen Gastgeber.

Fazit

Wer in die Sicherheit von Software investiert, investiert in das Vertrauen von Kundinnen und Kunden. Als Digitalisierungspartner mit langjähriger Expertise im Bereich IT-Security empfehlen wir eine Trilogie aus 1. der Sicherheit und Sicherung aller verwendeten Hard- und Softwarebestandteile, 2. die Unterstützung der Nutzerinnen und Nutzer mit sinnvollen Voreinstellungen, etwa bei der Authentifizierung, und 3. die ständige Beobachtung der Gefahrenlage im Netz inkl. Schaffung eines entsprechenden Bewusstseins und Verhaltens im eigenen Unternehmen. Wir beraten Sie gern! />

* https://de.statista.com/themen/1834/internetkriminalitaet/
**https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2020/Presse2020/200930_pmBLBCybercrime.html
***Trusted Information Security Assessment Exchange

AUF EINE TASSE JAVA MIT

Florian Heinecke

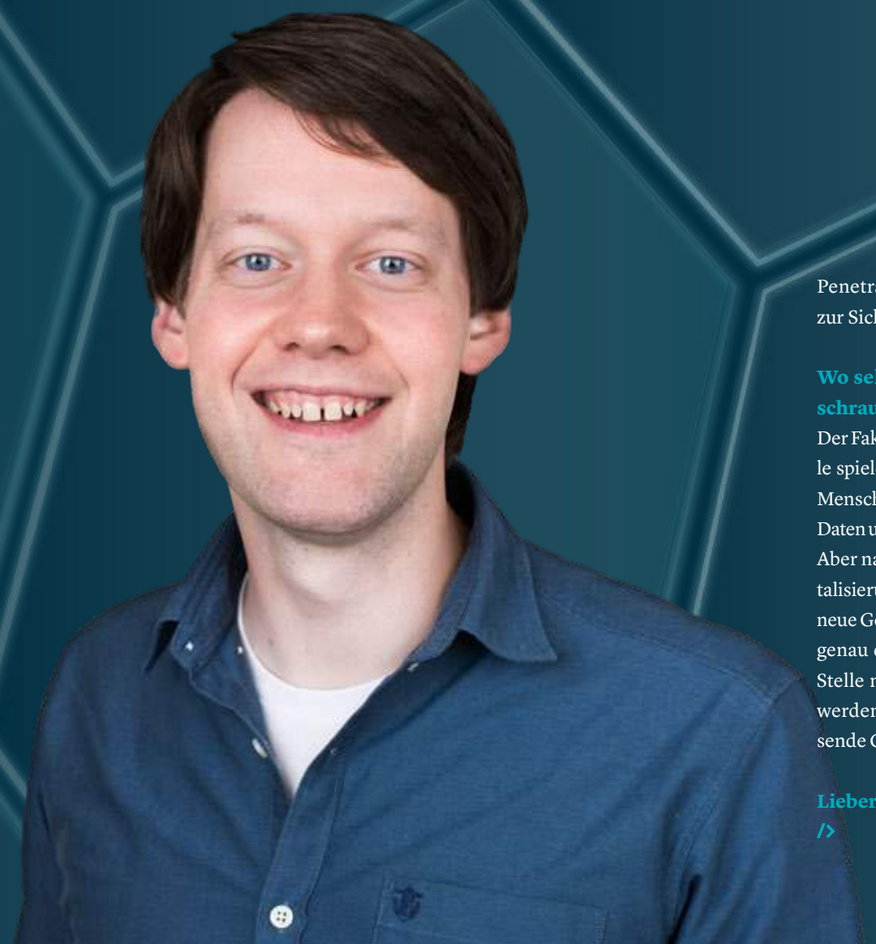
Informationssicherheit &
Datenschutz bei Micromata

Florian, ihr Ansprechpartner für IT-Security bei Micromata habt sicher alle Hände voll zu tun, oder?
Klar, in den letzten Jahren sind Cyberangriffe weltweit stetig mehr geworden. Unser Anspruch ist es deshalb, immer am Ball zu bleiben und der Gefahr fachlich und technisch stets einen Schritt voraus zu sein. Dabei setzen wir viel auf die Sensibilisierung unserer Teams, um die Erfolgsaussichten potenzieller Angriffe möglichst flächendeckend zu minimieren.

Was sind denn die häufigsten Cyberattacken? Kannst du sie kurz umreißen?
Wir beobachten eine zunehmende Professionalisierung von Angriffen allgemein, etwa im Bereich Phishing oder Ransomware. Zweck ist immer das Abfischen sensibler Daten und/oder das Lahmlegen ganzer Infrastrukturen, oft in Verbindung mit einer Lösegeldforderung. Und wenn die Systeme gut geschützt sind, versucht man es über die Schwachstelle Mensch. Das nennen wir dann Social Engineering. Viele Angriffe führen aber auch dann zum Erfolg, wenn Software nicht gepatcht wird oder Risiken nicht umfänglich geprüft und reduziert werden.

Wie lauten eure wichtigsten Tipps zum Schutz von Daten und Systemen?
Die Sensibilisierung für das Thema ist ein wichtiger erster Schritt. Das bedeutet, dass man neben den üblichen Schulungen die IT-Security auch in den Alltag integrieren sollte. Wir machen das z. B. über Security Champions in jedem Team, die eng mit uns zusammenarbeiten. Außerdem ist ein gutes Risikomanagement essenziell: mögliche Gefährdungen und Risiken identifizieren, die richtigen Maßnahmen daraus ableiten, schnell reagieren.

Wie ernst nehmen denn unsere Kunden das Thema?
Unsere Kunden sind als DAX-40-Konzerne und Global Player in Sachen IT-Sicherheit natürlich gut aufgestellt. Ein Beispiel dafür ist das im Titeltext genannte TISAX-Zertifikat der Automobilbranche. Von uns als IT-Dienstleister wird ebenfalls ein hohes Niveau erwartet und wiederkehrend evaluiert, dass wir die Grundsätze und Standards der jeweiligen Branchen einhalten. Außerdem führen wir im Auftrag unserer Kundinnen und Kunden regelmäßig



Penetrationstests durch und tragen so erheblich zur Sicherheit ihrer IT-Landschaften bei.

Wo seht ihr zukünftig die wichtigsten Stellschrauben in Sachen IT-Sicherheit?
Der Faktor Mensch wird weiterhin eine tragende Rolle spielen. Denn letztlich sitzt irgendwo immer ein Mensch, der durch sein Verhalten die Sicherheit von Daten und Systemen entweder schützt oder gefährdet. Aber natürlich werden sich mit zunehmender Digitalisierung auch neue Angriffsvektoren ergeben und neue Geschäftsmodelle für Cyberkriminelle. Welche genau das sein werden, darüber will ich an dieser Stelle nicht spekulieren. Aber wir von Micromata werden die Entwicklung genau beobachten, passende Gegenmaßnahmen erarbeiten und anbieten.

Lieber Florian, vielen Dank für das Gespräch!
/>

MODERN TALKING

–

Unsere Speaker auf
Online-Fachkonferenzen 2021

Vorsicht giftige Post!

Matthias Altmann

Digitaltag 2021
18. Juni 2021

Als Social Engineering bezeichnen wir den Versuch, die größte Sicherheitslücke überhaupt auszunutzen – uns Menschen. Die Einfallstore für diese Art krimineller Manipulation erstrecken sich von der Haustür über das Telefon bis hin zum E-Mail-Postfach.

Phishing & Co.

In diesem Workshop geht es darum, wie wir uns vor verseuchten E-Mails schützen können: Woran wir gefälschte Post erkennen, welche kriminellen Absichten dahinterstecken, wie wir sinnvoll darauf reagieren und wie wir uns auch vor uns selbst beschützen: vor unseren natürlichen Reflexen und unbewussten Verhaltensweisen, die manchmal schneller sind als der Verstand. Gemeint sind Pflichtgefühl, Hilfsbereitschaft, Angst oder Gier. Denn genau dies sind die Stellschrauben, wo Social Engineering ansetzt und wo wir besonders achtsam sein müssen.

Der Workshop richtet sich an alle, die das Netz regelmäßig nutzen und dort zur Zielscheibe von Social Engineering werden können. Denn auch wenn wir uns für kompetente Nutzer halten, können wir stets noch etwas dazulernen oder helfen, andere in unserem Umfeld vor dubiosen Machenschaften dieser Art zu schützen. />

Dieses Seminar ist bei Micromata on demand buchbar.

Clean Code steigert Softwarequalität: Endlich aufgeräumt!

Arkadius Roczniewski

IT-Tage 2021
07. Dezember 2021

Wie in einer Küche mit vielen Köchen arbeiten Entwickler Tag für Tag an einer gemeinsamen Codebasis, manchmal über Jahre hinweg.

Wer seinen Quellcode da nicht unter Kontrolle hat, bewegt sich rasant auf einen wirtschaftlichen Totalschaden zu, verursacht durch technische Schulden. Dieser Gefahr können wir mit Clean Code wirksam entgegenwirken. Denn mithilfe von Clean Code produzieren wir lesbaren und damit wartbaren Quellcode. So, dass jeder Entwickler sich leicht im Softwareprojekt zurechtfinden kann. Clean Code ist an sich nichts neues, jeder Entwickler weiß, dass er „eigentlich“ sauberen und lesbaren Code schreiben sollte. Aber werden wir diesem Anspruch in der Praxis immer gerecht?

In seinem Vortrag verdeutlicht Arkadius Roczniewski die Wichtigkeit von Clean Code und gibt einen unterhaltsamen und praxisnahen Einblick zu:

- den Folgen von unlesbarem Code und den Vorteilen von Clean Code
- den Basics der Clean-Coding-Regeln mit Beispielen und Best Practices
- der Rolle von Refactoring und Unit-Testing beim Clean Coding

/>

Spielerische Sicherheit

Matthias Altmann und
Claudius Link

XP Days
05. November 2021

Sicherheit ist ein großes Thema. Einerseits ist hier individuelle Verantwortung gefragt, andererseits auch tiefere Kenntnisse der Systems und Geschäftsprozesse. Hier ist dann Expertenwissen hilfreich.

Sicherheitsspiele ermöglichen es, verschiedene Aspekte der IT-Security kennenzulernen und diese im individuellen Geschäftsumfeld anzuwenden, ohne dass Fehler schwerwiegende Konsequenzen haben. Gleichzeitig ermöglichen sie es, vorhandenes Wissen im Team zu heben und implizites Wissen explizit zu machen. In diesem Workshop wurden zwei solcher Security Games vorgestellt. />

jugh!

TAGEBUCH 2. Halbjahr 2021

–

Alle JUGH-Talks auch auf Youtube:
youtube.com/MicromataTV

26. August 2021

Java 17 ist da!

In diesem Vortrag stellt Nicolai Parlog die neuen Sprachfeatures von Java 17 vor, neue bzw. aktualisierte APIs sowie neue JVM-Funktionen, die alle beim letzten Release eingeführt wurden. Diese haben nämlich einiges auf Lager. Der Vortrag verrät mehr über

- neue Sprachfunktionen wie versiegelte Typen, Pattern-Matching, Records, Switch-Ausdrücke und mehr
- Ergänzungen zu bestehenden APIs wie Stream und Optional
- andere Feinheiten wie Multi-Release-JARs und Leistungsverbesserungen

Wer sich das anschaut, ist anschließend bereit, mit Java 17 loszulegen! />

NICOLAI PARLOG
Java Developer Advocate
bei Oracle
@nipafx

30. September 2021

How to turn your monolith into a kick-ass cloud solution

Alle reden über Cloud und Microservices. Dabei fallen unvermeidliche Schlagworte wie Kubernetes, Prometheus, Graylog, CI/CD und so weiter …

Jetzt stehst du da, in diesem Buzzword-Hagel. Ohne Schirm und ohne Hut, aber dafür mit einem über Jahre gewachsenen Monolithen, der seinen Dienst noch immer gut macht. Wegwerfen? Auf keinen Fall! Behalten und veredeln? Unbedingt!

In diesem Talk zeigt uns Sebastian Hardt, wie wir eine vorhandene Codebasis aufmöbeln und erweitern können, um sie für eine Zukunft in der Cloud fit zu machen. Und zwar ohne alles über den Haufen werfen zu müssen. Wir sehen, wie man einen Monolithen in der Cloud zum Fliegen bringt! />

SEBASTIAN HARDT
Software Engineer
bei Micromata
@SebasthSeppel

28. Oktober 2021

Open Source CI/CD Components for GitHub Actions

GitHub Actions können jeden Workflow orchestrieren, ausgehend von den Ereignissen auf der GitHub-Plattform. In seinem Vortrag zeigt Lothar Schulz, wie wir eine CI/CD-Pipeline mit Open-Source-GitHub-Action-Komponenten implementieren. Und er stellt Open-Source-Initiativen vor, die auf GitHub Actions umsteigen. Außerdem können die Teilnehmer die vorgestellten Open-Source-Beispiele nutzen, um ihre eigenen CI/CD-Pipelines auf der Grundlage von Open-Source-GitHub-Action-Komponenten zu erstellen. />

LOTHAR SCHULZ
Freier Software Engineer
und Manager
@lothar_schulz

25. November 2021

Infrastructure as Code – Korrektheit beweisen statt testen

Gerd Aschemann zeigt uns, wie wir jQAssistant (jQA) dazu nutzen können, IaC-Definitionen zu scannen und zu analysieren, bevor wir sie ausrollen. Durch die Integration in unser Build-System wird damit jede Änderung semantisch geprüft und zurückgewiesen, sollten die definierten Constraints nicht erfüllt sein. Die Feedback-Loop verkürzt sich dadurch erheblich. Außerdem kann jQA auch Dokumentation und Reports erzeugen und prüfen. />

GERD ASCHEMANN
Freier Software Engineer
@GerdAschemann

Aus der Arbeit des IT-Security Meetups Kassel

Keine IT-Sicherheit ohne Know-how-Transfer

Das IT-Security Meetup Kassel ist ein Netzwerk von Experten und Interessierten zum Thema IT-Sicherheit. Eingeladen sind alle, die sich beruflich oder aus persönlichem Interesse mit Fragen der IT-Sicherheit auseinandersetzen und in einen fachlichen Austausch mit Gleichgesinnten treten wollen. Micromata ist Mitbegründer und Gastgeber des Meetups. Hier zwei aufgezeichnete Beispiele aus dem Programm.

DevSecOps in OWASP-Projekten
23. Juni 2021

Das Open Web Application Security Project (OWASP) macht es sich zur Aufgabe, die Sicherheit von Webanwendungen zu verbessern. Dazu widmet es sich zunehmend auch vielen DevSecOps*-Themen. Timo Pagel stellt in diesem Vortrag eine Auswahl an Projekten vor, an denen das deutschen OWASP-Chapter beteiligt ist. Darunter strategische Projekte wie DSOMM oder SAMM, aber auch Trainingssanwendungen wie Juice Shop oder Continuous-Security-Testing-Werkzeuge wie SecureCodeBox und DefectDojo. />

TIMO PAGEL
Freier IT-Security-Experte

**DevSecOps verknüpft Entwicklung, Security und den Betrieb von Software. Dabei werden Systeme und Methoden eingesetzt, die dafür sorgen, dass die Wahrscheinlichkeit von Schwachstellen und Sicherheitslücken entlang dieser ganzen Kette substanziell gemindert wird.*

Browser attacks on internal networks
14. Juli 2021

Angriffe aus dem Internet auf interne Unternehmensnetzwerke sind eine relative neue und deshalb noch wenig erforschte Gefahr. Die meisten Quellen beschreiben zwar die Ausnutzung von Protokollen aus dem öffentlichen Internet, aber so gut wie keine befasst sich mit lokal laufenden Diensten. Da Browser standardmäßig sowohl auf den Localhost als auch auf das lokale LAN zugreifen, überwinden solche Angriffe indes nicht nur die lokale, host-basierte Firewall, sondern auch die Perimeter-Firewall von Unternehmen mühelos. Dieser Vortrag von Michael Stevens beim IT-Security Meetup Kassel zeigt auf, wie solche Angriffe gestrickt sind und wie wir ihnen vorbeugen können. />

MICHAEL STEVENS
Software Engineer bei Micromata

Alle ITSM-Vorträge auch auf Youtube:
youtube.com/MicromataTV

2021

Hacktober fest

Coden statt schunkeln. Das jährliche Hacktoberfest lockt unsere Entwickler:innen nicht ins Wirtshaus oder Bierzelt, sondern auf die GitHub-Plattform: Quelltext teilen, Gemeinschaft pflegen, Spaß haben! Getreu dem Open-Source-Motto: Echter Fortschritt gelingt nur durch Know-how-Transfer.

Fotos: Kai Dorschner für Micromata

Spielend programmieren lernen

Codeweek Kassel 2021

Die Codeweek Kassel ist Teil einer europaweiten Initiative und lädt Menschen jedes Alters dazu ein, ihr Wissen zum Thema Software + Programmierung mit praktischen Lernangeboten zu verbessern. Ein buntes und niederschwelliges Programm soll die Teilnehmer:innen neugierig machen und ihnen ein Verständnis davon vermitteln, was Software eigentlich ist, wie sie funktioniert und was wir Tolles damit machen können.

Anna Klingauf, Softwareentwicklern bei Micromata, hat diesmal durch den Workshop geführt. *„Softwareentwicklung macht einfach riesigen Spaß“*, sagt sie. *„Weil wir so viele spannende Dinge damit tun können. Das Thema ist mittlerweile so unglaublich wichtig und erscheint so groß, dass viele Menschen sich gar nicht zutrauen überhaupt einzusteigen. In unserem Workshop zur Codeweek 2021 haben wir unsere Teilnehmer:innen auf ein kleines Software-Abenteuer mitgenommen und ihnen gezeigt, wie sie mit JavaScript auf spielerische Weise in diese Welt einsteigen können und wie viel Freude das bringt.“* />

Micromata fit für nachhaltige Zukunft

Alexander Podlich ist neuer Gesellschafter

Alexander Podlich, Geschäftsführer und „Micromata-Urgestein“ ist seit diesem Herbst neuer Gesellschafter des Unternehmens. Seine Beteiligung ist eine logische Folge aus vielen Jahren vertrauensvoller und zukunftsstiftender Zusammenarbeit. Begonnen hat sie für ihn 2007 zunächst als Softwareentwickler, von wo er sich rasch zum Projektleiter und dann zum BU-Leiter weiterentwickelte, um 2017 Teil der Geschäftsführung zu werden.

Wer Micromata ein wenig kennt, weiß: Nachhaltigkeit ist hier ein zentrales Anliegen. Im Hinblick auf Technologien ebenso wie im Hinblick auf die Beziehung zu den Kunden und den mittlerweile über 170 Mitarbeitenden. Im Fokus steht stets eine gleichermaßen wertschätzende wie wertschöpfende Unternehmenskultur, die ökonomische und menschliche Belange in Einklang zu bringen weiß. Aus dieser Überzeugung heraus hat Micromata auch immer auf Fremdkapital verzichtet und so die Abhängigkeit von externen Investoren vermieden.

Mit Alexander Podlich als neuem Gesellschafter wird diese Kultur kontinuierlich fortgeschrieben. „Ich freue mich sehr, dass mein Co-Geschäftsführer jetzt auch Sozius geworden ist“, so Kai Reinhard, CEO von Micromata. Damit verjüngen wir den Gesellschafterkreis und tragen weiter zur Zukunftsfähigkeit von Micromata bei.“

Selbst zu diesem Schritt befragt, antwortet Alexander Podlich mit folgenden Worten: *„Für mich ist Micromata schon immer mehr als nur ein Job. Es ist die Möglichkeit, die Digitalisierung für unsere tollen Kunden und Partner intelligent, kreativ und mutig mitzugestalten. Und es ist überdies eine bunte Gemeinschaft ganz außergewöhnlicher Menschen voller Begeisterung und Passion für ihre Themen, mit denen ich sehr gern zusammenarbeite und jeden Tag erlebe.“* />

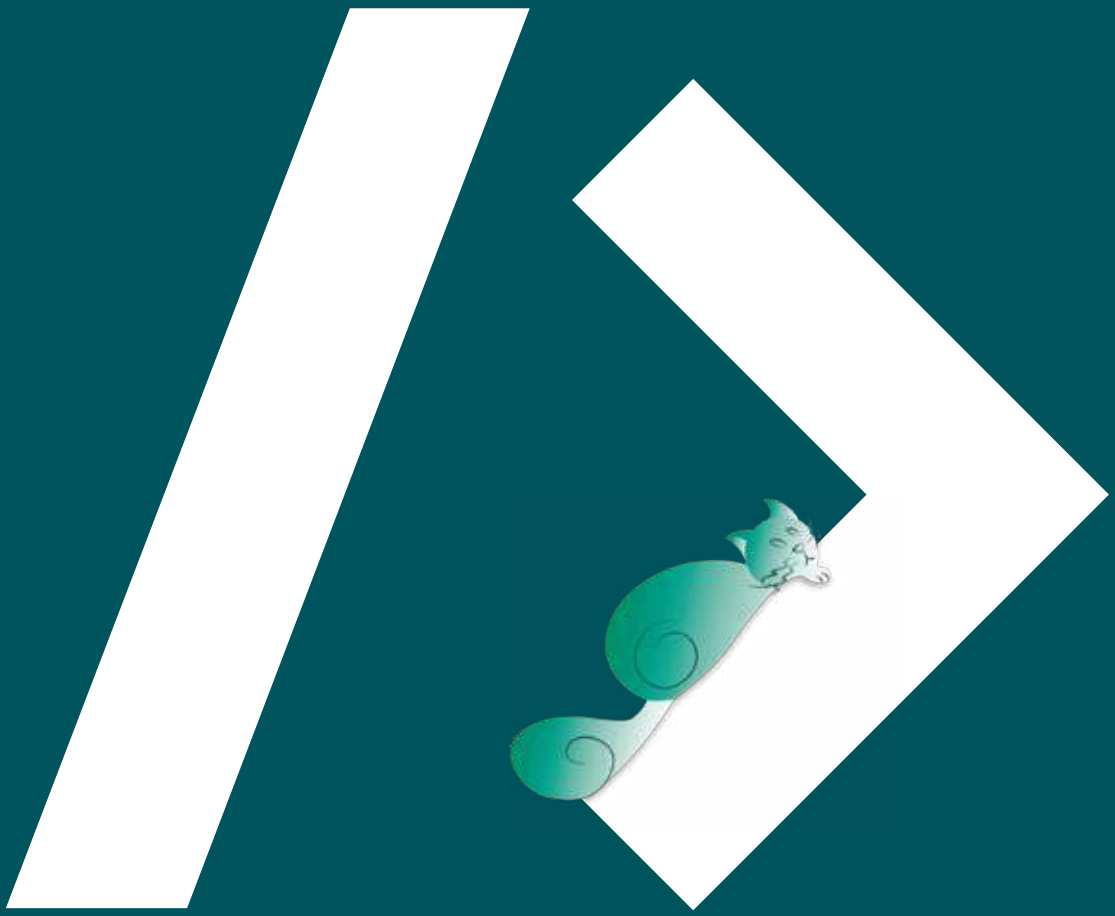
3 x Zukunft für junge IT-Talente

Micromata finanziert drei Deutschland-stipendien für Informatik-Studierende

Die Universität Kassel ist dieses Jahr 50 Jahre alt geworden. Als Alma Mater vieler unserer Mitarbeitenden, darunter auch unserer Geschäftsführer Kai Reinhard und Alexander Podlich, fühlen wir uns der Hochschule noch immer freundschaftlich verbunden. Schließlich hat sie nicht unerheblich zum Erfolg von Micromata beigetragen - und tut es noch heute. Grund genug, mal unsere Wertschätzung auszudrücken.

„Die Digitalisierung ist eines der wichtigsten Themen unserer Zeit. Damit sie gelingt, brauchen wir die besten Köpfe. Die Uni hilft uns, sie zu finden und auszubilden - gemeinsam machen wir uns schon seit vielen Jahren für den IT-Nachwuchs stark. Deshalb haben wir den 50. Geburtstag der Uni Kassel einfach mal zum Anlass genommen, am Fachbereich Informatik/Elektrotechnik drei Deutschland-stipendien zu finanzieren. Wir freuen uns!“
Alexander Podlich, Geschäftsführer bei Micromata

Das Deutschlandstipendium ist eine deutschlandweite Initiative des Bundesministeriums für Bildung und Forschung (BMBF), das von den Hochschulen organisatorisch betreut und von privaten Unternehmen finanziell gefördert wird. Ziel ist es, junge Talente zu fördern, den Übergang vom Studium in den Beruf zu verbessern und dem Fachkräftemangel entgegenzuwirken. />



Wenn Sie das Quelltext-Magazin nicht mehr erhalten möchten, schreiben Sie uns eine Mail an marketing@micromata.de

HERAUSGEBER
Micromata GmbH
Marie-Calm-Straße 1-5
34131 Kassel

FON +49 561 31 67 93-0
www.micromata.de

V.i.s.d.P. Kai Reinhard
REDAKTION
Jule Witte

TITELBILD Clara Höferlin
LAYOUT + SATZ Machbar GmbH
DRUCK Boxan
Gedruckt auf FSC®-zertifiziertem Papier