Bits & Matjes – „Cyberattacken“

Am 17. Oktober 2024 fand im Digitalen Innovationszentrum Greifswald (DIZ Greifswald) die Veranstaltung "Bits & Matjes" statt – ein etabliertes Angebot zur Förderung der Digitalisierung im Kreis Vorpommern Greifswald. Die Veranstaltung, die durch das DIZ Greifswald und in Kooperation mit dem Landkreis Vorpommern-Greifswald, der Industrie- und Handelskammer Neubrandenburg (IHK), der Handwerkskammer Ostmecklenburg-Vorpommern der Bundesagentur für Arbeit Greifswald durchgeführt wird, brachte von 12:00 bis 14:00 Uhr Unternehmer:innen, Digitalisierungsinteressierte und Expert:innen zusammen. Ziel war es, die digitale Transformation in der Region voranzutreiben und die regionale Wirtschaft zu stärken. Mit einer gelungenen Mischung aus praxisnahen Fachvorträgen, Beratung und Networking bot die Veranstaltungsreihe ein spannendes, informatives und inspirierendes Programm, das darauf abzielte, Unternehmen, Gründer:innen und Interessierte im Bereich der digitalen Transformation zu unterstützen und zu vernetzen.

"Bits & Matjes" findet monatlich statt und deckt ein breites Spektrum digitaler Themen ab. Das Format besteht aus zwei Hauptkomponenten. Die Veranstaltung beginnt mit Impulsvorträgen von Expert:innen und Präsentationen zu aktuellen digitalen Trends und Technologien. Die anschließende Netzwerkphase dient dazu, bei einem kleinen, informellen maritimen Imbiss (symbolisiert durch das namensgebende "Matjes") Kontakte zu knüpfen und Erfahrungen auszutauschen. Diese Struktur fördert sowohl den Wissenstransfer als auch die Bildung von Kooperationen zwischen verschiedenen Akteuren der regionalen Wirtschaft.

Vollständig vom Land Mecklenburg-Vorpommern gefördert, bietet das DIZ Greifswald beratende Leistungen für Unternehmen im Digitalisierungsprozess, Impulse für innovative digitale Lösungen und ein umfangreiches Netzwerk für den Austausch zwischen verschiedenen Akteuren. Das DIZ fungiert somit als treibende Kraft für die digitale Transformation in der Region.

Der Themenschwerpunkt der aktuellen Veranstaltung konzentrierte sich auf „Cyberattacken“.

Cybersicherheit in der Praxis – Andreas Thiel, Clausohm-Software GmbH

Andreas Thiel von der Clausohm-Software GmbH führte die Teilnehmer durch die vielfältigen Facetten der Cybersicherheit und stellte gezielte Maßnahmen vor, die insbesondere für kleine und mittlere Unternehmen (KMU) relevant sind:

1. **Kontinuierliche Schutzmaßnahmen**: Clausohm setzt auf *Continuous Protection* und bietet unter anderem Penetrationstests und Schwachstellenanalysen an. Das *Monitoring as a Service* ist ein zentraler Service, der Unternehmen hilft, ihre Systeme kontinuierlich auf potenzielle Bedrohungen zu überwachen.
2. **Sicherheitsüberprüfungen und Red Teaming**: Clausohm führt Sicherheitsüberprüfungen mit simulierten Angriffen durch, um Schwachstellen in IT-Infrastrukturen aufzudecken. *Red Teaming* ermöglicht, durch gezielte Angriffe und *Social Engineering*-Taktiken die Sicherheitsvorkehrungen eines Unternehmens realitätsnah zu testen.
3. **Phishing-Kampagnen und Schulungen**: Simulierte *Phishing-Mail-Kampagnen* helfen, Mitarbeitende für diese Art von Cyberangriffen zu sensibilisieren. Clausohm

setzt zusätzlich auf eine eigens entwickelte Awareness-Plattform, die Mitarbeitende schult und vorbereitet.
4. **Einsatz Künstlicher Intelligenz (KI)**: KI wird bei Clausohm zur Erstellung täuschend echter Phishing-Mails genutzt, die es ermöglichen, Schwachstellen in der menschlichen Wahrnehmung zu identifizieren und das Bewusstsein für Bedrohungen weiter zu schärfen.
5. **Beratung zu Sicherheitsrichtlinien**: Clausohm unterstützt Unternehmen bei der Einführung eines Informationssicherheits-Management-Systems (ISMS), das strategisch in Sicherheitsrichtlinien und Notfallmanagement (BCM) eingebettet ist. Für KMU stellt dies eine praktikable Herangehensweise dar, um Cybersicherheitsmaßnahmen nachhaltig zu implementieren.

Innovative Authentifizierungsmethoden – Viktor Garske, Institut für sichere mobile Kommunikation an der Hochschule Stralsund

Viktor Garske vom Institut für sichere mobile Kommunikation an der Hochschule Stralsund widmete sich in seinem Vortrag dem Thema moderner Authentifizierungsmethoden und stellte *Passkeys* als zukunftsweisende Alternative zu Passwörtern vor:

1. **Hintergrund zu Passwörtern**: Garske begann mit einem historischen Überblick und erklärte, wie Passwörter seit den 1960er-Jahren zur Authentifizierung genutzt werden. Problematisch ist, dass Passwörter anfällig für Phishing und andere Angriffe sind.
2. **Passkeys als sichere Alternative**: Passkeys basieren auf einem Schlüsselpaar, das mit dem Domainnamen einer Website verknüpft ist und somit nicht durch Phishing kompromittiert werden kann. Diese Schlüssel werden sicher auf dem Endgerät oder einem Authentifizierungs-Token gespeichert und nur nach erfolgreicher Verifizierung freigegeben.
3. **Implementierung und Vorteile**: Für die Nutzung von Passkeys ist die „Web Authentication API“ (WebAuthn) erforderlich. Garske betonte, dass diese Technologie benutzerfreundlicher und sicherer ist als Passwörter und bereits von großen Anbietern wie Google und Apple unterstützt wird.
4. **Kritische Betrachtung**: Garske wies darauf hin, dass Passkeys viele Phishing-Risiken eliminieren, aber auch einige Einschränkungen aufweisen. Zum Beispiel sind Passkeys an ein bestimmtes Gerät gebunden und erfordern häufig die Integration von Cloud-Diensten zur Synchronisation.

IT-Sicherheit im Hochschulkontext – Gordon Grubert, Universitätsrechenzentrum Greifswald

Gordon Grubert, der technische Leiter des Rechenzentrums der Universität Greifswald, erläuterte die Herausforderungen und Strategien, mit denen Hochschulen wie die Universität Greifswald ihre IT-Infrastrukturen absichern:

1. **Risikoanalyse und Bedrohungsbewertung**: Grubert betonte, dass die Universität potenziellen Cyberbedrohungen gut gerüstet gegenübertritt. Die größten Gefahren gehen von ungesicherten IT-Infrastrukturen aus, die wie ein „Kartenhaus“ zusammenfallen können, wenn zentrale Komponenten wie Active Directory kompromittiert werden.
2. **Ebenenübergreifende Sicherheitsstrategie**: Ein zentrales Element der Sicherheitsstrategie ist die Verwendung von offenen Standards und dezentralen Lösungen. Das Netzwerk, die Anwendungen und das Identitätsmanagement (IdMS) werden so strukturiert, dass der Ausfall einer Komponente nicht die gesamte Infrastruktur gefährdet. Grubert stellte einen Failover-Plan vor, der den Ausfall zentraler Systeme in kürzester Zeit beheben kann.
3. **Honeypot-Strategie zur Ransomware-Prävention**: Um Ransomware-Angriffe zu erkennen, setzt die Universität Honeypots auf dem Fileserver ein. Diese Fallen registrieren unautorisierte Zugriffe und leiten sofort Gegenmaßnahmen ein, wie z. B. die Sperrung der Angreifer-IP und betroffener Nutzenden.
4. **Benutzerfreundliche Sicherheitsmaßnahmen**: Grubert verwies auf die Bedeutung benutzerfreundlicher, aber konsequenter Sicherheitsmaßnahmen wie Zwei-Faktor-Authentifizierung (2FA) für VPN-Zugänge. Auch wenn dies für manche Nutzer unbequem erscheint, ist es ein essenzieller Schritt, um die Sicherheit der universitären IT-Infrastruktur zu gewährleisten.

Fazit

Die Veranstaltungsreihe "Bits & Matjes" hat sich als ein wirksames Forum zur Förderung der Digitalisierung im Landkreis Vorpommern-Greifswald etabliert. Die praxisnahen Vorträge von ExpertInnen wie Andreas Thiel, Viktor Garske und Gordon Grubert bieten einen tiefen Einblick in die Herausforderungen und Lösungen rund um die Cybersicherheit und digitale Transformation. Mit der Fokussierung auf Wissenstransfer, Anwendungsbeispiele und Netzwerkbildung stärkt "Bits & Matjes" die digitale Kompetenz der Region und trägt aktiv zur digitalen Innovationsstrategie von Mecklenburg-Vorpommern bei.