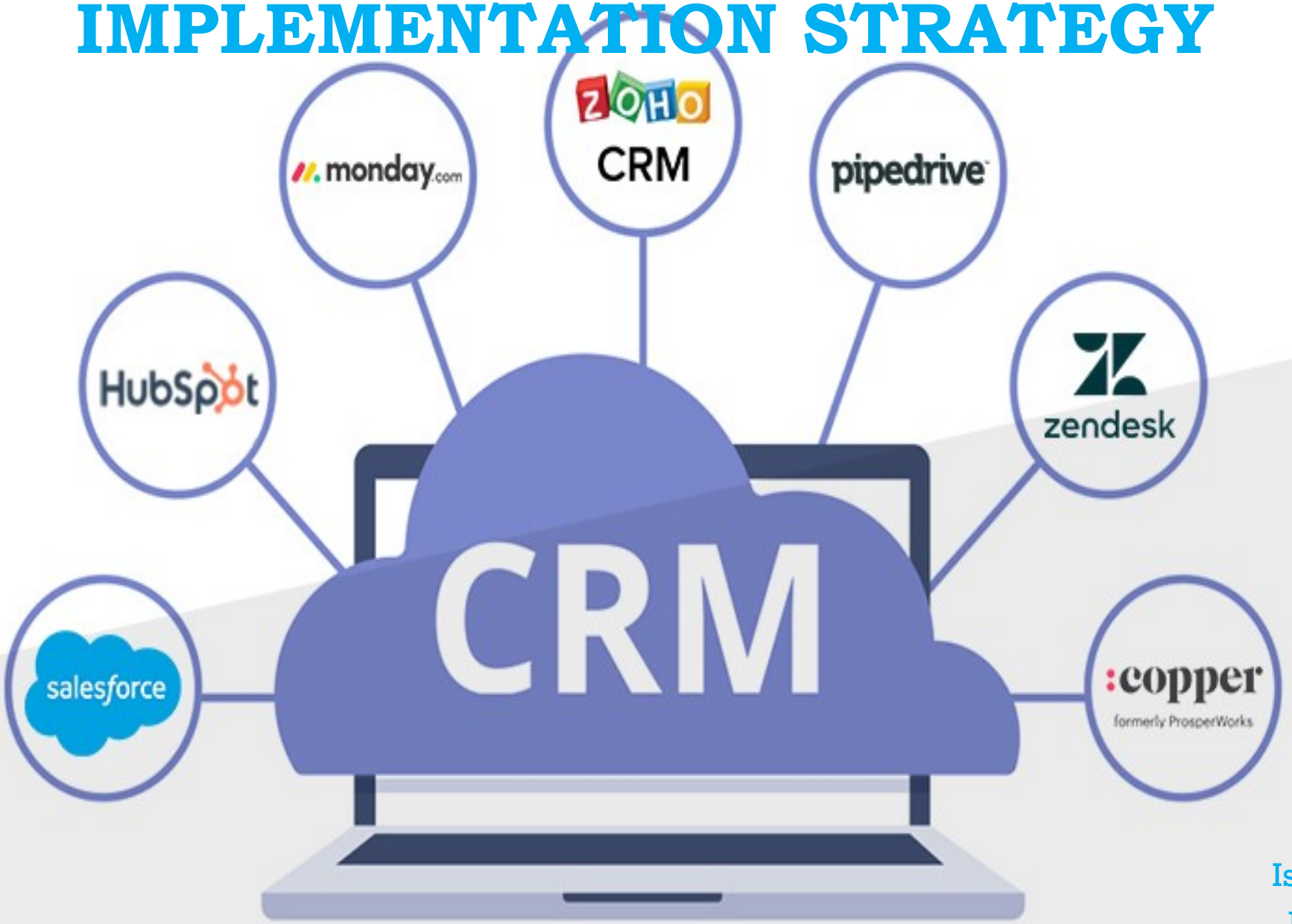
ZERO TRUST ARCHITECTURE (ZTA) IMPLEMENTATION STRATEGY



Easton Soares
Ismail Mahamed
Jaskaran Sohal
Rayyan Khan

TABLE OF CONTENTS

- Data Security in CRM: ZTA Perspective Slide 3
- Application Security within CRM: ZTA Approach Slide 4
- Asset Management in CRM under ZTA Slide 5
- Ensuring Service Integrity in CRM with ZTA Slide 6
- References Slide 7

DATA SECURITY IN CRM: ZTA PERSPECTIVE

Types of Data in CRM:

- Customer data often includes sensitive personal information, preferences, and interaction history.
- Transaction histories encompass sales records, service subscriptions, and billing information.
- Communication logs can contain email exchanges, chat histories, and call recordings.
- Analytics data may include customer behavior patterns, sales forecasts, and marketing campaign results.

Risks and Challenges:

- Unauthorized access could occur via weak authentication systems or insider threats.
- Data breaches might be the result of targeted cyber-attacks, such as phishing or ransomware.
- Compliance issues arise from not adhering to laws and standards that govern data protection and privacy.

Encryption:

- Data-at-rest encryption ensures that stored data is unreadable without proper authorization.
- Data-in-transit encryption protects data as it moves between networks or devices, preventing interception or eavesdropping.

Access Controls:

- Role-based access control (RBAC) restricts system access to authorized users based on their role within the organization.
- The principle of least privilege limits user access rights to only what is necessary to perform their job.
- Multi-factor authentication (MFA) requires multiple methods of verification before granting access, adding an extra layer of security.

Data Monitoring:

- Continuous monitoring involves real-time analysis of network traffic and user activities to detect suspicious behavior.
- Anomaly detection uses machine learning and statistical analysis to identify deviations from normal behavior patterns.
- Regular audits are systematic examinations of records and activities to ensure compliance and security standards are met.

Compliance Considerations:

- The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU).
- The California Consumer Privacy Act (CCPA) gives California residents new rights regarding their personal information and aims to enhance privacy rights and consumer protection.

APPLICATION SECURITY WITHIN CRM: ZTA APPROACH

Application Security Landscape

Cloud-Based CRM Vulnerabilities: CRM systems hosted on the cloud have potential weak points such as exposed APIs, insecure data storage, or misconfigured access controls. Complex, multi-tenant cloud environments can increase the risk of cross-site scripting (XSS), injection attacks, and other exploits.

ZTA Security Measures

- **Secure Coding**:
  - **Practices**: Include the use of coding standards that prevent common vulnerabilities, such as the OWASP Top Ten, and the implementation of code review processes.
  - **Tools**: Utilize industry-leading code analysis tools such as SonarQube for continuous static code inspection and Fortify for in-depth vulnerability detection, alongside dynamic application security testing with tools like OWASP ZAP and Burp Suite to ensure our web applications are robust against security threats.
  - **Training**: Emphasize the importance of developer training in secure coding practices.
- **Application Firewalls**:
  - **Types**: Application firewalls, such as network-based, host-based, and cloud-based, and their use cases.
  - **Functionalities**: Deep packet inspection, heuristic analysis, and signature-based detection to block malicious traffic.
- **Regular Security Audits**:
  - **Vulnerability Assessments**: The process of identifying, quantifying, and prioritizing vulnerabilities in the CRM system.
  - **Penetration Testing**: The simulated cyber-attack against your CRM system to check for exploitable vulnerabilities.
  - **Audit Frequency and Depth**: Audits should be conducted quarterly and delve into the system's architecture.
- **User Authentication and Authorization**:
  - **Biometric Authentication**: The use of fingerprint, facial recognition, or other biometric methods to verify user identities.
  - **Behavior Analytics**: Monitoring user behavior to detect anomalies that could indicate a security breach.
  - **Continuous Verification**: The ongoing process of verifying the security of a session or transaction, not just at the login stage.

ASSET MANAGEMENT IN CRM UNDER ZTA

Defining CRM Assets

- **Physical Assets**: These are tangible resources such as servers and user devices. They are critical to CRM operations and must be physically secured.
- **Digital Assets**: Include software, databases, and the data contained within the CRM. This also covers the network infrastructure that supports the CRM, like routers and switches, and application components such as web servers and middleware.

ZTA Asset Protection Strategies

- **Device Hardening**:
  - **Endpoint Configuration**: Remove unnecessary services, close unused ports, and ensure systems are configured according to industry best practices.
  - **Security Layers**: Implement firewalls, antivirus, and intrusion detection systems (IDS) on endpoints to prevent exploitation.
  - **Regular Reviews**: Periodically review device configurations to ensure they remain secure against evolving threats.
- **Updates and Patch Management**:
  - **Vulnerability Tracking**: Maintain an inventory of assets and monitor for known vulnerabilities.
  - **Patch Testing and Deployment**: Test patches in a controlled environment before widespread deployment to ensure they do not introduce new issues.
  - **Automation**: Utilize automated tools to deploy patches to ensure timely updates across all assets.
- **Asset Monitoring and Response**:
  - **Real-time Monitoring**: Utilize Splunk for its advanced capabilities in monitoring, searching, and analyzing machine-generated big data through a web-style interface.
  - **Incident Response**: Implement IBM's Resilient Incident Response Platform (IRP) to streamline and orchestrate the incident response process, ensuring rapid action and recovery from incidents.
  - **Forensics and Analysis**: Deploy EnCase by Guidance Software for comprehensive forensic analysis, allowing detailed investigation and the uncovering of potential security breaches.
- **Lifecycle Management**:
  - **Procurement to Disposal**: Track the asset from procurement, through its working life, to its eventual disposal, ensuring that security is a consideration at each stage.
  - **Regular Auditing**: Conduct regular audits to assess the effectiveness of asset management processes.
  - **Continuous Improvement**: Use the insights gained from monitoring and audits to continually refine lifecycle management practices.

ENSURING SERVICE INTEGRITY IN CRM WITH ZTA

CRM Services Overview

- **APIs**: These are the set of protocols and tools for building application software and facilitating communication between different software intermediaries.
- **Web Services**: Services offered through the web using technologies like XML, JSON, REST, and SOAP to enable operation across different machines and systems.
- **Cloud-based Functionalities**: These refer to CRM features and services that are hosted on cloud infrastructure, offering scalability, flexibility, and accessibility.

ZTA for Service Protection

- **API Security**:
  - **Authentication Protocols**: Implement protocols like OAuth for token-based authentication and OpenID Connect for identity verification.
  - **API Gateways**: Use API gateways to manage, authenticate, and route API traffic, applying consistent security policies across all services.
- **Service-Level Authentication**:
  - **Robust Mechanisms**: Utilize multi-factor authentication, certificates, and biometrics to ensure only authorized entities can access services.
  - **Authorization Policies**: Define and enforce strict access control policies that determine what authenticated users are allowed to do within the CRM services.
- **Continuous Monitoring**:
  - **24/7 Monitoring Tools:** Implement Nagios for round-the-clock surveillance of our CRM services, ensuring real-time insights into system health, performance, and security alerts.
  - **Methodologies**: Adopt a practice that includes regular security scanning, logging, and anomaly detection to identify and respond to threats promptly.
- **High Availability Strategies**:
  - **Redundancy**: Ensure that critical components of the CRM services have redundant systems in place to take over in case of failure.
  - **Load Balancing**: Distribute workloads across multiple servers to ensure optimal service performance and availability.
  - **Disaster Recovery Plans**: Develop and regularly test disaster recovery plans to ensure CRM services can be quickly restored after any outage.

REFERENCES

- [1] Q. Yao, Q. Wang, X. Zhang, and J. Fei, "Dynamic Access Control and Authorization System based on Zero-trust architecture," Journal Name, pp. 123-127, doi: 10.1145/3437802.3437824. [Online]. Available: https://dl.acm.org/doi/10.1145/3437802.3437824. Accessed on: Nov. 23, 2023.

- [2] J.Poole, "Mutual TLS: Microservices Encryption for Service Mesh," TheNewStack, Month Day, Year. [Online]. Available: https://thenewstack.io/mutual-tls-microservices-encryption-for-service-mesh/. Accessed on: Nov. 23, 2023.

- [3] J. Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," Forrester, [Online]. Available: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf. Accessed on: Nov. 23, 2023.