MADE BY:APARNA MISHRA AND STEFAN

DETAILED NOTES ON NETWORK SEGMENTATION

JULY 2, 2024

Overview

Introduction to Network Segmentation:

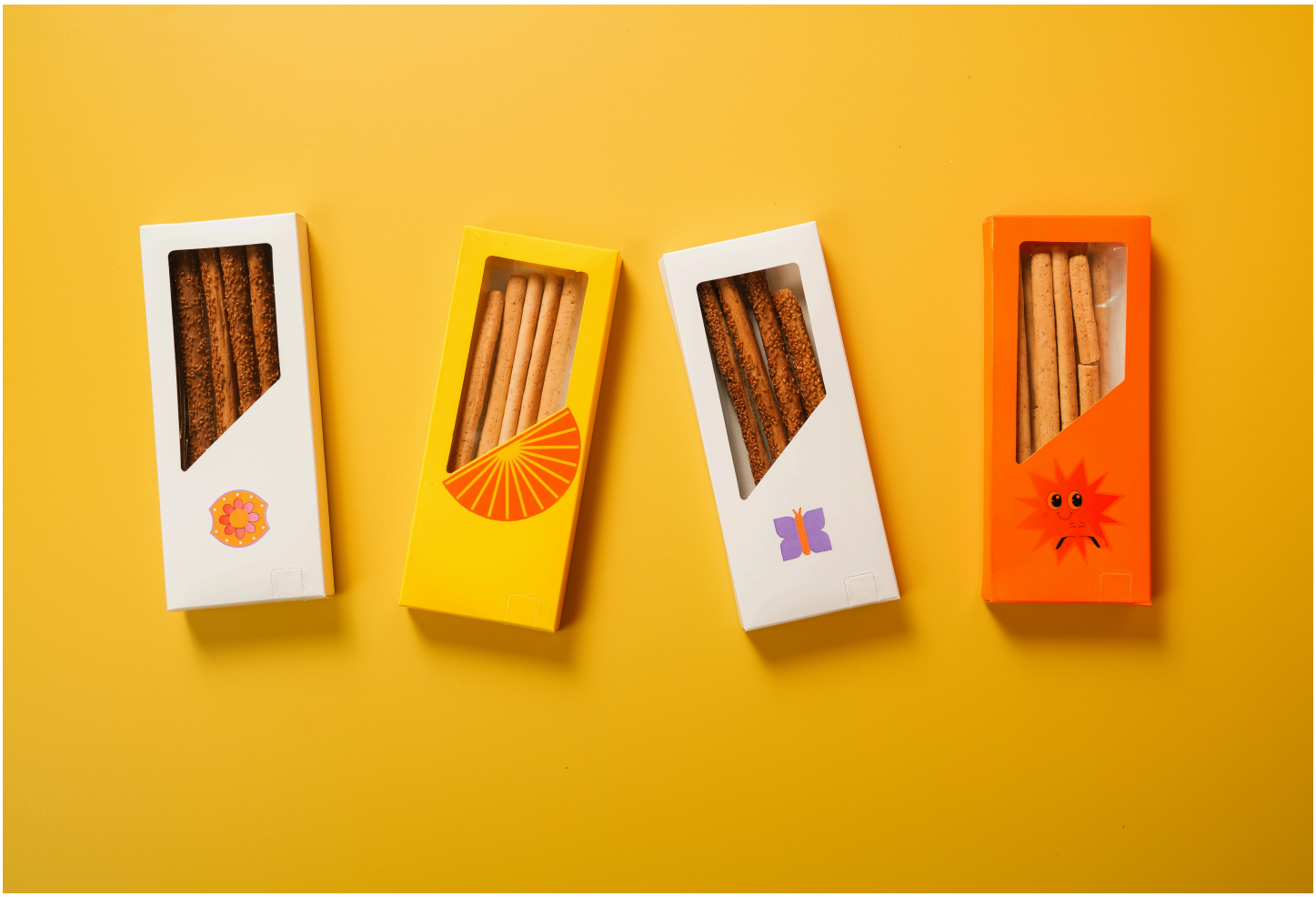
Network segmentation involves dividing a computer network into smaller, isolated networks or segments. Each segment, or zone, contains specific types of devices and services, such as servers, clients, and administrative resources. This segregation enhances security by limiting the impact of potential breaches and controlling network traffic more effectively.

Contributions of Segmentation to Network Security:

1. **Isolation of Critical Assets:**
   - By placing critical assets in separate segments (e.g., servers in a Server Zone), segmentation limits the exposure of these assets to potential threats originating from other parts of the network. This reduces the risk of lateral movement by attackers.
2. **Controlled Access:**
   - Segmentation enables fine-grained access control policies based on the sensitivity and function of each segment. For example, a Client Zone may have stricter outbound traffic rules compared to a Server Zone.
3. **Reduced Attack Surface:**
   - By dividing the network into segments, organizations can minimize the overall attack surface. This makes it harder for attackers to compromise multiple segments if one segment is breached.
4. **Improved Performance and Management:**
   - Segmentation can improve network performance by reducing broadcast traffic and optimizing resource allocation. It also facilitates easier network management and troubleshooting.
5. **Compliance and Regulatory Requirements:**
   - Many compliance standards (e.g., PCI DSS) require segmentation as a security best practice to protect sensitive data and ensure regulatory compliance.

Security of the Whole Organization:

- Effective network segmentation doesn't just protect individual segments but enhances the overall security posture of the organization. It ensures that even if one segment is compromised, the rest of the network remains secure, preventing widespread damage and data loss.



KNJ Label's visual branding peg

Configuration of Firewalls at Boldi AG

Network Segmentation Overview Provided by Head of IT Infrastructure:

- **Domain:** Logical division of network objects.
- **Admin Zone:** Special purpose servers (e.g., SIEM).
- **Server Zone:** Application and database servers.
- **Client Zone:** User laptops.

Firewall Configuration Approaches:

1. **Whitelisting vs. Blacklisting:**

- **Whitelisting:** Allows only pre-approved traffic based on predefined rules. It specifies what is explicitly allowed, reducing the risk of unauthorized access and malware infections. This approach is more secure but requires careful planning and maintenance of rule sets.
- **Blacklisting:** Blocks known malicious traffic based on predefined lists. It is less secure as it may not catch all threats, especially zero-day exploits or unknown malware variants. However, it can be more flexible for environments with frequently changing needs.

Configuration Recommendations for Firewalls A, B, C, and D:

- **Firewall A (Domain Zone):**
  - **Whitelisting:** Allow only necessary domain-related traffic (e.g., Active Directory).
  - **Reason:** Protects domain integrity and prevents unauthorized access to directory services.
- **Firewall B (Admin Zone):**
  - **Whitelisting:** Permit access only to authorized administrative tools and services (e.g., SIEM).
  - **Reason:** Ensures centralized logging and monitoring without exposing administrative resources to unnecessary risks.
- **Firewall C (Server Zone):**
  - **Whitelisting:** Configure rules to allow specific traffic required for applications and databases.
  - **Reason:** Protects critical server resources from unauthorized access and potential data breaches.
- **Firewall D (Client Zone):**
  - **Blacklisting:** Block known malicious websites and malware command-and-control traffic.
  - **Reason:** Provides flexibility to handle potentially risky user behavior and emerging threats not covered by whitelisted rules.