Kiteworks

www.kiteworks.com

Personal Data in the Crosshairs: Takeaways From Verizon's 2023 DBIR

Mitigating Sophisticated Email Attacks and Protecting Against Human Error

Humans and Personal Data

74%

of Breaches Include a Human Element (error, privilege misuse, stolen credentials, social engineering)

Over **50%**

of Incidents Targeted Personal Data (PII, PHI, Other)

Breach Highlights

83%
of Breaches Involved External Actors

49%
of Breaches Involved Credentials

24%
of Breaches Involved Ransomware

Content Being Targeted

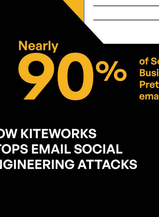
87%
Personally Identifiable Information (PII)

30%
Protected Health Information (PHI)

21%
Other

13%
Bank

Email Attacks Become More Sophisticated



Nearly **90%** of Social Engineering Attacks Are Business Email Compromise (BEC) Pretexting (leverage existing email threads)

HOW KITEWORKS STOPS EMAIL SOCIAL ENGINEERING ATTACKS

- Uses a closed, invitation-only email system to which attackers cannot send social engineering attacks
- Scans email with integrated antivirus, ATP, and CDR
- Employs digital fingerprinting to verify attachment integrity
- Uses multi-factor authentication to protect against credential attacks

Misdelivery and Publishing Errors Spike Upward

43%

of Errors Are Misdelivery:
Data shared with someone other than the intended person or when something was sent to an unknown destination

HOW KITEWORKS PROTECTS AGAINST MISDELIVERY

- **Secure Email:** Encrypts messages and attachments, ensuring only intended recipients can access the content, and enables sensitive files to be withdrawn in an email when sent to the wrong recipient.
- **Granular Access Control:** Set specific access permissions for each user, reducing the risk of sensitive information being accidentally shared or sent to unauthorized individuals.
- **Built-in Audit Logs:** Detailed record of all user activities that makes it easier to identify and address misdelivery issues.
- **Role-based Policies:** Establish and enforce policies based on user roles to ensure sensitive data is only accessible to those who need it.
- **Secure Shared Folders:** Create secure folders for sharing sensitive information so that only authorized users can access the content.
- **Compliance Reporting:** Monitor and maintain compliance with data protection regulations to reduce the risk of misdelivery incidents.

23%

of Errors Are Publishing Errors:
Data is sent to the wrong audience

HOW KITEWORKS PROTECTS AGAINST PUBLISHING ERRORS

- **Secure Storage:** Secure environment for storing sensitive content that reduces the risk of accidental publishing or unauthorized access.
- **Version Control:** Track changes and revert to previous versions of a document if a publishing error does occur.
- **Access Controls:** Set granular access permissions for each user to ensure that only authorized individuals can edit, send, and share sensitive content.
- **Workflow Management:** Create and manage workflows for content review and approval to prevent publishing errors (viz., reviewed by appropriate users before it is published).
- **Audit Logs:** Detailed record of all user activities to make it easier to identify and address publishing errors.
- **Real-time Monitoring:** Quickly detect and respond to potential publishing errors when they do occur.

For more Kiteworks Insights on Verizon's 2023 DBIR, check out our blog post.

For more on the Kiteworks Private Content Network, click here.