Black Friday Edition

BLUVIT

GUIDE

CYBER WEEKS

Ist Ihr Unternehmen wirklich *sicher?*

DAS RISIKO,
FRÜHERKENNUNG
& SCHUTZMASSNAHMEN

www.bluvit.de | 0561 9402 6666 | service@bluvit.de

Das Risiko lauert im Homeoffice.

DIE BLACK FRIDAY WEEK IST DIE GEFÄHRLICHSTE PHISHING-SAISON DES JAHRES.

Die Zeiten, in denen Betrug leicht an schlechter Grammatik erkennbar war, sind vorbei.

Durch den Einsatz von Künstlicher Intelligenz (KI) erstellen Kriminelle täuschend echte Repliken von Websites (Spoofing) und formulieren Phishing-Mails, die von legitimer Geschäftskommunikation kaum zu unterscheiden sind.

Häufige Probleme

- Mitarbeiter suchen auf Arbeitsgeräten nach privaten Angeboten oder öffnen vermeintliche "Corporate Benefit"-Mails.
- Gefälschte Angebote für Büroausstattung oder Software-Lizenzen locken Einkaufsabteilungen.
- Kriminelle kopieren Ihren Webshop oder Ihre Corporate Identity, um Dritte zu betrügen, was massive Reputationsschäden zur Folge hat.

Digitale Fallen erkennen

SENSIBILISIEREN SIE IHRE TEAMS FÜR FOLGENDE INDIKATOREN:

Die Mechanismen der Betrüger zielen auf psychologische Trigger, die auch im B2B-Kontext funktionieren.

Anomalien in der URL (Typosquatting)

Betrüger registrieren Domains, die legitimen Marken zum Verwechseln ähnlich sehen, um Login-Daten abzugreifen oder Malware zu verteilen.

- **Beispiel:** Statt www.apple.com wird www.appple.com oder www.apple-blackweek-deals.com genutzt.
- **Business-Risk:** Ein Mitarbeiter gibt seine Microsoft-365-Zugangsdaten auf einer gefälschten Login-Seite ein, die ihm einen "Black Friday Rabatt" für Software verspricht.

Social-Media-Betrugsfallen

Bei künstlicher Verknappung (Zeitdruck, limitierte Stückzahl) setzt das kritische Denken aus.

- **Warnsignal:** "Zahlung muss innerhalb von 2 Stunden erfolgen, um den 80% Rabatt auf die neuen Laptops zu sichern."
- **Business-Risk:** Umgehung etablierter Freigabeprozesse im Einkauf durch suggerierte Dringlichkeit.

Inkonsistente Geschäftsangaben

Hochprofessionelle Fake-Shops nutzen KI-generierte AGBs und gefälschte Impressen.

- **Warnsignal:** Fehlende Handelsregistereinträge, nicht klickbare Gütesiegel (z.B. Trusted Shops) oder Zahlungsaufforderungen an Konten im Ausland trotz deutscher Adresse.
- **Business-Risk:** Überweisung von Vorkasse an Scheinfirmen; Erhalt von Plagiaten oder minderwertiger IT-Hardware, die Sicherheitsrisiken bergen kann.

Die Bezahlmethoden-Täuschung

Viele professionelle Fake-Shops bauen Vertrauen auf, indem sie im Footer oder auf der Produktseite Logos von seriösen Zahlungsdienstleistern (PayPal, Visa, Klarna, Rechnungskauf) präsentieren.

- **Der Trick:** Der Bestellprozess läuft bis zum letzten Schritt normal. Erst beim Klick auf "Kaufen" erscheint eine Fehlermeldung (z. B. "Derzeit technische Störung bei Kreditkartenzahlung" oder "API-Limit erreicht"). Dem Käufer wird suggeriert, die einzige verbleibende Option sei die Echtzeitüberweisung oder Vorkasse, um den Deal nicht zu verlieren.

Strategische Schutzmaßnahmen für Unternehmen

IT-Sicherheit ist kein Zustand, sondern ein Prozess. Nutzen Sie die Black Week als Anlass, um Ihre Sicherheitsarchitektur und Awareness zu härten.

Technische Maßnahmen

DNS-FILTER & WEB-SECURITY	Blockieren Sie den Zugriff auf bekannte Phishing-Domains und neu registrierte Domains (die jünger als 30 Tage sind) im Firmennetzwerk.
E-MAIL-GATEWAY-HÄRTUNG	Verschärfen Sie die Spam-Filter-Regeln für den Zeitraum November/Dezember. Aktivieren Sie Warnhinweise für E-Mails, die von externen Absendern kommen.
BRAND MONITORING	Überwachen Sie das Web proaktiv auf neu registrierte Domains, die Ihren Markennamen enthalten, um Typosquatting frühzeitig zu erkennen und Takedowns einzuleiten.

Organisatorische Maßnahmen & Compliance

Untersagen Sie "Schatten-IT-Käufe". Bestellungen dürfen nur bei vorvalidierten Lieferanten (Whitelisting) getätigt werden.	**STRENGE BESCHAFFUNGS-RICHTLINIEN**
Implementieren Sie Richtlinien, die Vorkasse bei neuen, unbekannten Lieferanten während der Black Week kategorisch ausschließen. Nutzen Sie Zahlungsziele oder Treuhanddienste.	**VERBOT VON VORKASSE BEI ERSTKONTAKTEN**
Fordern Sie bei neuen Anbietern immer einen Handelsregisterauszug und eine Umsatzsteuer-ID-Prüfung an.	**VALIDIERUNG**

Human Firewall (Mitarbeiter-Sensibilisierung)

AWARENESS FÖRDERN	Informieren Sie Mitarbeiter proaktiv über die Zunahme von Phishing-Mails, die als Paketbenachrichtigungen (DHL/FedEx) oder "Sonderangebote für Mitarbeiter" getarnt sind.
TRENNUNG VON BERUFS- UND PRIVATLEBEN	Erinnern Sie daran, dass privates Online-Shopping auf Firmengeräten die Sicherheitsarchitektur gefährdet.
SOCIAL MEDIA SKEPSIS	Weisen Sie Marketing- und HR-Teams an, keine Links in Werbeanzeigen auf LinkedIn oder Instagram ungeprüft zu öffnen – auch B2B-Plattformen sind vor Malvertising (schädlicher Werbung) nicht sicher.

Vorsicht ist besser als *Nachsicht*

Wir sind Ihr Partner für IT-Sicherheit

Haben Sie Bedenken bezüglich der Sicherheit Ihrer Einkaufs-Prozesse oder möchten Sie Ihre Mitarbeiter durch Awareness-Trainings auf die Black Week vorbereiten?

Dann besuchen Sie jetzt unsere Website oder rufen Sie einfach an. Wir beraten Sie gerne.

www.bluvit.de

0561 9402 6666 | service@bluvit.de