ONSEC

YOUR CASINO'S WEAKEST LINK

Third-Party Vendor Breaches in iGaming

ONSEC

They Didn't Hack the Casino

September 2023. MGM Resorts. $100 million in losses. The attackers didn't breach MGM's core systems directly. They compromised a vendor. Then pivoted inside.

Your casino is only as secure as your least secure vendor.

Payment processors. Game providers. CRM platforms. Loyalty program vendors. Every integration is an attack surface. Every third party is a potential entry point.

The iGaming Vendor Ecosystem

Why gambling platforms are uniquely exposed:

Integration complexity

- 50+ third-party integrations typical
- Payment gateways (multiple)
- Game aggregators
- KYC/AML providers
- Odds feed suppliers
- Affiliate platforms

Data sharing requirements

- Player PII shared with vendors
- Financial data transmitted
- Betting history exposed
- KYC documents stored externally

Real-time dependencies

- Live betting requires instant feeds
- Payment processing 24/7
- Game providers always connected
- Single vendor outage = platform down

Recent iGaming Vendor Breaches

The pattern is clear:

Incident	Vector	Impact
MGM/Caesars 2023	IT vendor social engineering	$100M+ losses
Fast Track CRM 2025	CRM platform breach	600K player records
Multiple operators 2024	Payment processor compromise	Financial fraud
Game provider breach 2024	Aggregator API exploitation	Multi-operator exposure

ONSEC

Attack Vectors Through Vendors

How attackers exploit the supply chain:

Credential compromise

- Vendor employee phishing
- Weak vendor authentication
- Shared service accounts
- API key theft

Software supply chain

- Malicious updates pushed
- Compromised SDKs
- Backdoored integrations
- Dependency hijacking

Network pivoting

- VPN connections exploited
- Trusted network access
- Lateral movement
- Privilege escalation

Data exfiltration

- Vendor database access
- Backup compromise
- Log file exposure
- API data harvesting

The Game Provider Risk

Specific to iGaming:

Integration depth

- Direct database connections
- Real-time data streams
- Player session access
- Financial transaction hooks

Multi-tenant exposure

- One provider, hundreds of casinos
- Shared infrastructure
- Common vulnerabilities
- Cascading breaches

Regulatory data

- Player verification data
- Responsible gambling flags
- Self-exclusion information
- Transaction records

Payment Processor Vulnerabilities

Critical iGaming dependency:

What they access

- Player financial data
- Transaction histories
- Withdrawal requests
- Bank account details

The risk

- Fraudulent transactions
- Data theft
- Service disruption
- Regulatory violations

Recent incidents

- Processor breaches affecting multiple operators
- Credential theft enabling fraud
- API vulnerabilities exploited
- Insider threats at processors

Vendor Security Assessment

What to evaluate:

Security posture

- SOC 2 Type II certification
- ISO 27001 compliance
- PCI DSS (if payment)
- Penetration test results

ONSEC

Access controls

- Authentication methods
- Privilege management
- Audit logging
- Separation of duties

Incident response

- Breach notification SLA
- Communication protocols
- Remediation capabilities
- Insurance coverage

Data handling

- Encryption standards
- Retention policies
- Deletion procedures
- Cross-border transfers

ONSEC

Questions for Your Vendor Management

Critical queries:

→ Do we have a complete inventory of all vendors with platform access?

→ What player data does each vendor access?

→ When did we last review vendor security certifications?

→ How quickly must vendors notify us of breaches?

→ Can we terminate vendor access immediately if needed?

→ Do we audit vendor access logs?

→ What's our liability if a vendor breach exposes player data?

Contractual Protections

What your vendor agreements need:

Security requirements

- Specific standards mandated
- Regular assessment rights
- Penetration testing requirements
- Compliance certifications

Breach obligations

- Notification timeframes (24-48 hours)
- Cooperation requirements
- Remediation responsibilities
- Liability allocation

Audit rights

- On-demand security audits
- Access to assessment results
- Remediation verification
- Ongoing compliance monitoring

Termination clauses

- Security breach triggers
- Data return/destruction
- Transition assistance
- Post-termination obligations

Technical Controls

Limiting vendor exposure:

ONSEC

Network segmentation

- Vendor-specific network zones
- Limited lateral movement
- Firewall restrictions
- Zero trust architecture

Access management

- Least privilege access
- Time-limited credentials
- Multi-factor authentication
- Session monitoring

API security

- Rate limiting
- Input validation
- Token-based auth
- Activity logging

Monitoring

- Vendor activity tracking
- Anomaly detection
- Real-time alerting
- Forensic logging

ONSEC's Vendor Risk Assessment

We evaluate your third-party exposure:

Vendor inventory

- Complete mapping
- Access documentation
- Data flow analysis
- Risk categorization

Security assessment

- Vendor security review
- Certification verification
- Gap identification
- Risk quantification

Control evaluation

- Technical controls audit
- Contractual review
- Process assessment
- Monitoring capability

Recommendations

- Risk mitigation priorities
- Contract improvements
- Technical hardening
- Ongoing monitoring

Your casino's security perimeter extends to every vendor.

The CRM that stores player data. The payment processor handling withdrawals. The game provider connected to your platform. Each one is an extension of your attack surface.

When they're breached, you're breached. When their data leaks, your players are exposed.

Key Takeaway:

MGM didn't get hacked. Their vendor did. The distinction didn't matter to players. Or regulators. Or the $100 million loss.

How well do you know your vendors' security?

About ONSEC

ONSEC is a boutique penetration testing and security assessment team specializing in iGaming platforms. We help operators identify vulnerabilities in APIs, payment systems, and player-facing applications before attackers do—whether the risk is fraud, data exposure, or regulatory non-compliance. Our team has worked with casinos, sportsbooks, and gaming providers across multiple jurisdictions. If you'd like to discuss how we can help strengthen your platform, reach out to schedule a quick call.

Our Services:

✓ Penetration Testing — Full-scope security assessments of your platform, APIs, and mobile apps

✓ iGaming Security Audits — Compliance-focused reviews for UKGC, MGA, and other regulators

✓ Fraud & AML Assessment — Evaluate your defenses against bonus abuse, multi-accounting, and money laundering

✓ Incident Response — 24/7 support when security incidents occur

✓ Security Architecture Review — Design secure systems from the ground up

✓ Dark Web Monitoring — Track your brand and player credentials on underground markets

https://onsec.io • request@onsec.io

ONSEC.io — Razor-Sharp Security for iGaming

Trusted by leading organizations worldwide.