Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

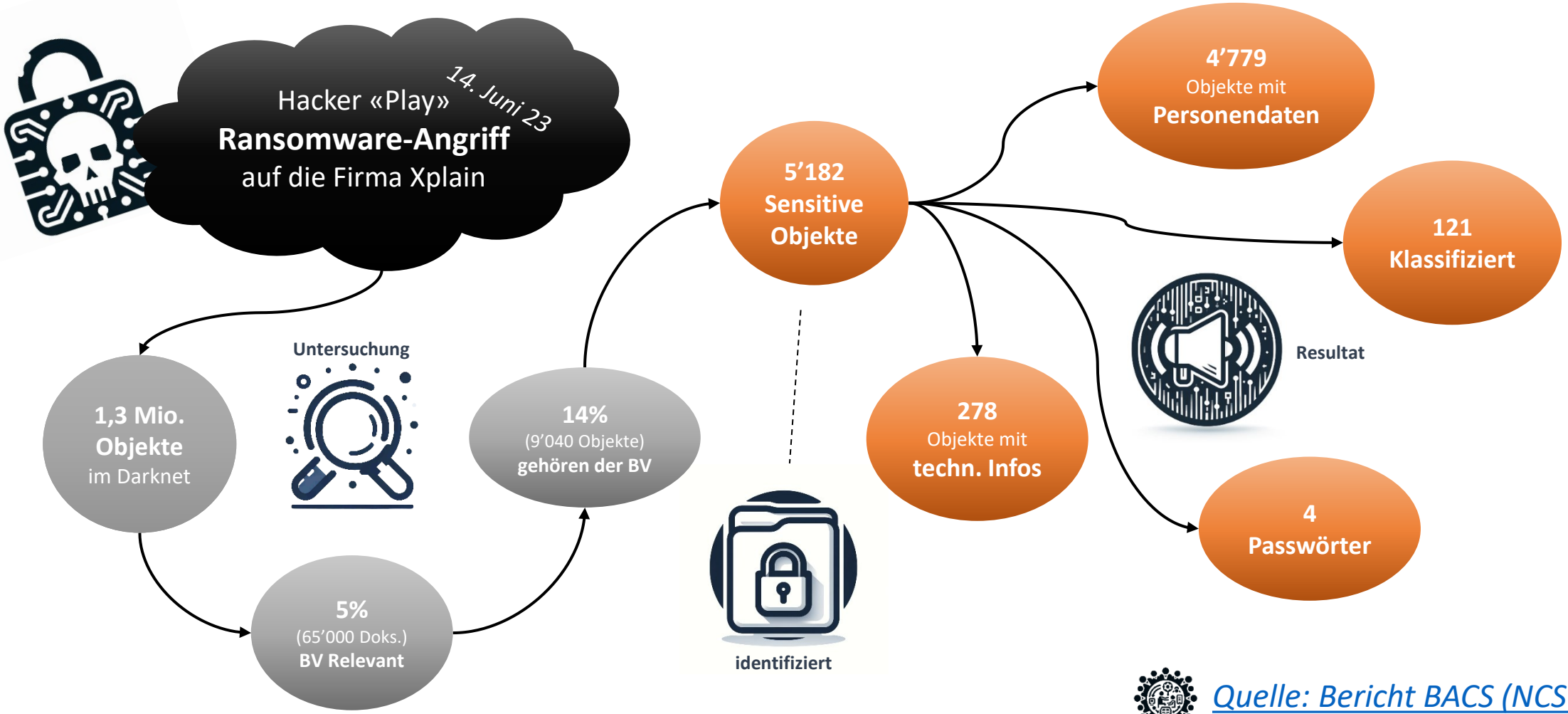
Eidgenössisches Finanzdepartement EFD
Bundesamt für Bauten und Logistik BBL

Hack to Basics:

Risikomanagement in der öffentlichen Beschaffung

6. Juni 2024 - Daniel Lüchinger

Basierend auf einer Wahren Geschichte



Quelle: Bericht BACS (NCSC)

Fokus: Beschaffung und Vertragsmanagement

Von der Krise zur Kontrolle

Jedes Projekt mit einem Lieferanten basiert auf einem **Beschaffungsvorhaben**, das durch einen **Vertrag** festgelegt wird.

Wer ist betroffen?
Was wurde beschafft?
Wie und wann wurde beschafft?

*Die **zentrale Beschaffungsstelle** sichert rechtliche und kommerzielle Standards, während die **Bedarfsstellen** für die Lieferantenbeziehungen und die Einhaltung technischer sowie sicherheitsrelevanter Anforderungen verantwortlich sind.*

Sofortmassnahmen und Reaktionen

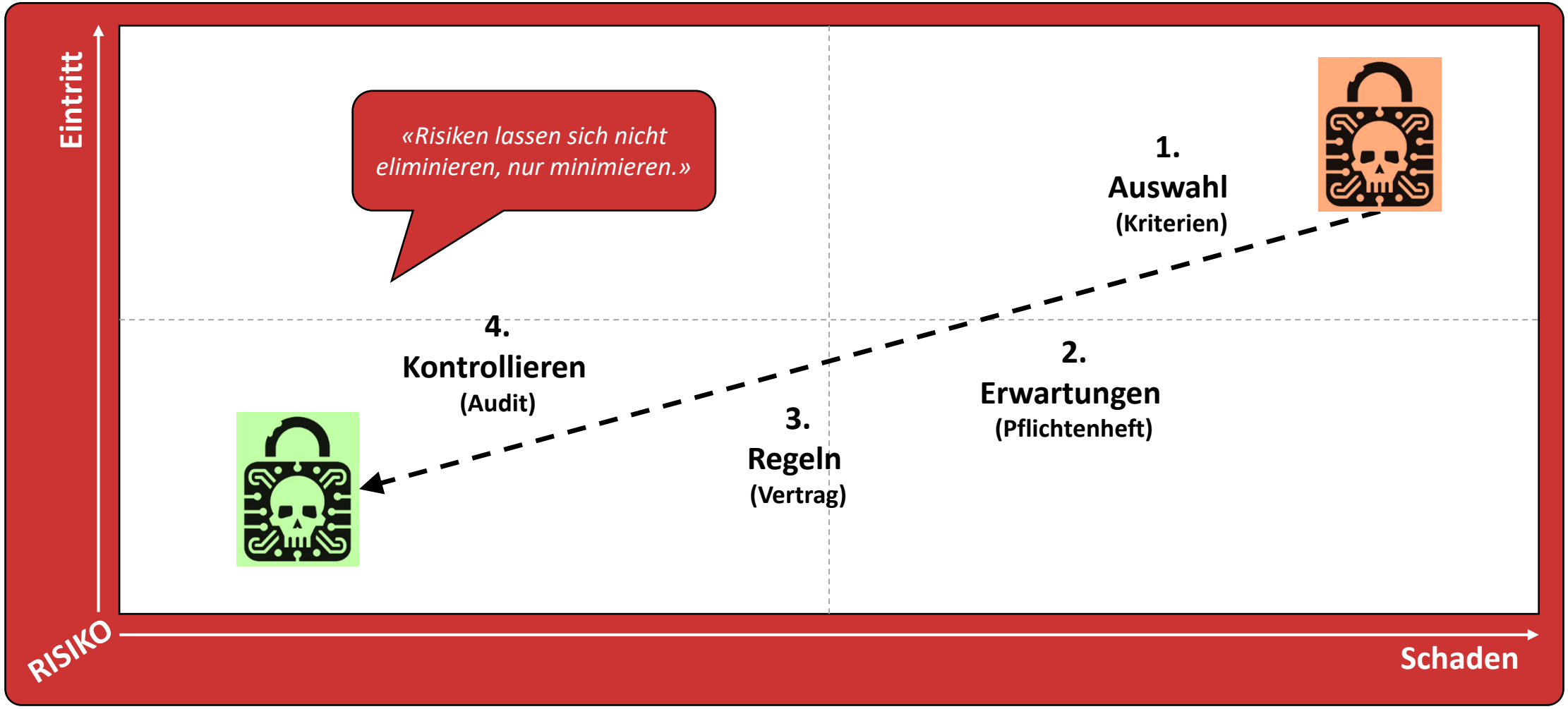
wie die zentrale Beschaffungsstelle unterstützen konnte

- **Informationsbereitstellung:** Dank einem gutem Beschaffungs-controlling und Vertragsmanagement konnten die Fragen WER, WAS, WIE & WANN innert Stunden beantwortet werden.
- **Escrow-Abkommen:** Gewährleistung der fortlaufenden kritischen Dienste und Software durch Absicherung mit Xplain.
- **Lösungsszenarien bei Konkurs:** Entwicklung von Notfallplänen zur Leistungssicherung für den Fall eines Konkurses von Xplain.
- **Rechnungsmanagement:** Überprüfung und Ausgleich offener Rechnungen zur Vermeidung finanzieller Engpässe mit Xplain.
- **Aktive Medienkommunikation:** Klare und proaktive Kommunikationsstrategien zur Vermeidung von Fehlinformationen und zur korrekten Darstellung der Sachlage (inkl. BGÖ).

Notiz: *In solchen Fällen soll die Zusammenarbeit zwischen Lieferant und Bund funktionieren. In diesem Fall ist die Firma Xplain seinen Pflichten nachgekommen.*

Risikosteuerung in der Beschaffung

Massnahmen zur Minimierung von Eintritt und Schaden



Effektivität und Grenzen von Beschaffungs-prozessen und Vertragsmanagement

- Verträge und Beschaffungsvorhaben können die Frage der Schuld nicht direkt klären, aber wichtige Details dazu liefern.
- Die Wahl des Vergabeverfahrens (offen oder freihändig) beeinflusst nicht die IT-Sicherheit; die Beschaffungsform ist nicht relevant.
- Verträge allein schützen nicht vor menschlichem Fehlverhalten; sorgfältiges Informationsmanagement bleibt unerlässlich.
- Verträge und standardisierte Beschaffungsprozesse allein können Angriffe durch organisierte Kriminelle, wie die Hackergruppe Play, nicht eliminieren oder verhindern.

Lehren aus dem Vorfall

Verstärkung der Sicherheitsmassnahmen

"Alle notwendigen Massnahmen sind vorhanden – es kommt darauf an, sie konsequent anzuwenden und in die Praxis umzusetzen."

Lieferantenmanagement: Obwohl ein Lieferantenmanagement in der zentralen Beschaffungsstelle etabliert wurde, zeigt der Vorfall, dass weitere Aufmerksamkeit und Ressourcen erforderlich sind, um seine Effektivität zu verstärken.

Personalsensibilisierung: Die Bundesverwaltung führt bereits verpflichtende Schulungen durch, jedoch ist eine Intensivierung der Sensibilisierungsmassnahmen notwendig, um menschliches Fehlverhalten weiter zu reduzieren.

Regelungen: Trotz der Einführung der Mustervertragsklausel der BKB zu Cyberrisiken im Jahr 2020 bedürfen bestehende Verträge, die noch auf Standards von 2003 basieren, einer verstärkten Überprüfung und Anpassung an aktuelle Anforderungen.

Audits: Grundlagen für effiziente Lieferantenaudits werden aufgebaut, um eine enge Verbindung zum Lieferantenmanagement zu gewährleisten.

…und deshalb Hack to Basics

Zurück zu den Grundlagen:

Risikomanagement *ist* ***Handeln*** *(****Verb****), nicht nur* ***Benennen*** *(****Nomen****)*

Die drei Ks **– *Kommandieren*** *(klare Anweisungen geben),* ***Kontrollieren*** *(fortlaufende Überprüfung),* ***Korrigieren*** *(schnelle Anpassungen vornehmen)*

Die ***Anerkennung*** *des* ***Top-Managements*** *sowie das tägliche* ***Bewusstsein jedes Einzelnen***

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Infos: Abschluss der Administrativuntersuchung zum Hackerangriff auf die Xplain AG: Bundesrat beschliesst Massnahmen